Installing and Upgrading the Avaya G430 Media Gateway

03-603233
Issue 2
November 2009

© 2009 Avaya Inc.
All Rights Reserved.

Notice

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

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

http://www.avaya.com/support

Copyright

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

Avaya support

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

http://www.avaya.com/support

Contents

About this book 11
Downloading this book and updates from the Web 11
Downloading this book 11
Safety labels and security alert labels 11
Related resources 13
Technical assistance 14
Within the US. 14
International 14
Trademarks. 14
Sending us comments 15

Chapter 1: Before you install 17
Before going to site 17
Preparing required equipment 17
Equipment required for installation 17
Equipment required for mounting 17
Equipment required for installing an S8300 Server 17
Equipment required if you are not installing an S8300 Server 18
Obtaining the G430 serial number 18
Obtaining RFA access. 18
Checking license file and Avaya Aura™ Communication Manager versions for a Local Survivable Processor (LSP) 19
Downloading CM license and authentication files to your laptop 19
Running the Automatic Registration Tool (ART) for the RAS IP address. 20
Obtaining the RAS IP address and password 20
Downloading recent firmware. 21
Obtaining the Electronic Preinstallation Worksheet (EPW). 21
Site requirements 22
Environmental verification 22
Power verification 22
Grounding verification 22
G430 package contents. 23
EM200 package contents 23
Unpacking and checking package contents 24

Chapter 2: Installing the Avaya G430 Media Gateway and EM200 25
Step 1: Mounting the G430 chassis 25
Mounting the G430 in a rack 25
Brackets without cable guides 26

Brackets with cable guides 26
Attaching each mounting bracket to the G430. 27
Before mounting the G430 27
Mounting the G430 in the rack 27
Mounting the G430 on a wall 28
Attaching brackets to the G430 for wall mounting 28
Fastening the G430 to the wall 29
Placing the G430 on a table 29
Step 2: Mounting the EM200 expansion module(s) 29
Step 3: Connecting EM200 expansion modules to the G430 30
Step 4: Installing the media modules. 30
Before inserting media modules into the G430 or EM200 chassis 31
Combination limitations 31
Allocating slots 31
Inserting the S8300 Server 33
Inserting media modules 35
Attaching ground conductors 37
General grounding requirements 37
Installation location 37
Ground conductor 37
Ground block. 38
Restricted Access Location 38
Approved grounds 38
Connecting the safety ground 40
Attaching the ground wires 40
Step 7: Connecting power to the EM200 expansion modules 41
Step 6: Connecting power to the G430 41

Chapter 3: Connecting devices. 43
Step 1: Connecting data and voice devices 43
Connecting a switch or a network data port 43
Connecting a computer to the Services port 43
Connecting an IP telephone. 44
Connecting the telephone to the G430 44
Connecting an ISDN BRI station 44
Connecting one ISDN BRI station to one ISDN port 45
Connecting two ISDN BRI stations to one ISDN port 45
Connecting an analog telephone 46
Connecting a DCP telephone to an MM712 or MM717 media module 48

Connecting an analog trunk 49
Analog trunk 49
Analog DID trunk 49
Connecting an E1/T1 trunk 50
Connecting an ISDN BRI trunk 50
Connecting devices to the MM717 and MM716 media modules 51
Connecting the MM716 or MM717 front panel connector to a punch down block 51
Step 2: Installing circuit protection 52
Step 3: Connecting to the Wide Area Network (WAN) 53
Connecting an Ethernet WAN link 53
Connecting an external router to the G430 53
Step 4: Installing the Coupled Bonding Conductor 53
Installing the CBC 54
Step 5: Installing the Avaya Partner Contact Closure Adjunct 54
Installing the contact closure 54

Chapter 4: Connecting and enabling a USB modem for remote access. 55
Connecting and enabling a USB modem (G430 without S8300) 55
Testing the modem connection (G430 without S8300) 57
Connecting and enabling a USB modem (G430 with S8300) 57
Maintenance web pages 57
Changing the modem settings on the Configure Server Maintenance Web Page 57
Connecting and enabling a USB modem (G430 with S8300) 58
Connecting and enabling the modem 58
Testing the modem connection (G430 with S8300) 59
If a USB CD-ROM drive is required to download software upgrades 59

Chapter 5: Configuring the G430 61
Configuring basic gateway connectivity 61

Chapter 6: After installation. 63
Step 1: Testing the installation 63
Testing data connectivity 63
Testing telephones 63
Testing trunks 63
LSP failover testing 64
Step 2: Removing the installation equipment 66

Chapter 7: Adding media modules and devices. 67
Adding a media module 67
Adding voice modules. 67
Adding a telephone 67
Connecting the telephone. 67
Configuring the telephone on the Communication Manager 68
Recording telephone information for software configuration 68
Testing the telephone 68
Adding a trunk 68
Ordering the trunk 69
Special considerations when ordering an analog trunk 69
Connecting the trunk 69
Configuring the trunk on CM 69
Recording trunk information for software configuration 70
Testing the trunk. 70
Adding a Broadband Line (xDSL or cable modem) 70
Ordering the Broadband line 70
Connecting the Broadband line. 71
Configuring the Broadband line on the G430 71
Testing the Broadband link 71
Adding an Avaya Partner Contact Closure Adjunct 71

Chapter 8: Upgrading and replacing Field Replaceable Units 73
Inserting or removing an MP10, MP20 or MP80 VoIP module 73
Removing the G430 cover. 73
Inserting a VoIP module 75
Removing a VoIP module 77
Replacing the G430 cover 77
Installing the upgrade memory kit 79
Replacing a RAM card. 79
Replacing the RAM card. 79
Inserting or removing a compact flash memory card 80
Inserting a compact flash memory card 80
Removing a compact flash memory card 81

Chapter 9: Upgrading the G430 firmware 85
Upgrading G430 firmware using Avaya Software Update Manager 85
Upgrading G430 firmware from the primary controller 85
Upgrading G430 firmware using Gateway Installation Wizard (GIW). 86

Upgrading G430 firmware using Avaya Installation Wizard (IW) 86
Upgrading G430 firmware using the CLI via FTP/TFTP 88
CLI commands for upgrading G430 firmware via FTP/TFTP 88
Example upgrade via FTP/TFTP using the CLI 89
Preparing installation worksheets 89
Entering values in Server Values worksheet. 90
Setting up a TFTP server 91
Downloading G430 firmware files to a local TFTP server 91
Installing firmware from the TFTP server on the S8300 Server. 92
Copying firmware files to the */tftpboot* directory of an S8300 Server . . . 93
Upgrading G430 firmware using the CLI via a USB device 93
CLI Commands for upgrading G430 firmware via a USB device 94
Example upgrade using the CLI via a USB device 94
Downloading G430 firmware files to a local PC 94

Chapter 10: Upgrading IP phone configuration and firmware files . . . 97
Administering the upgrade 98
Upgrading the IP telephone 99
TFTP IP telephone upgrade examples 101
Upgrading the 4602SW and 4602D phones 101
Upgrading 4620 IP phones 103
Failure scenarios and repair actions 104
Upgrading considerations 105

Chapter 11: Backing up and restoring the G430 107

Chapter 12: Troubleshooting 109
One telephone stops working. 109
Identifying the problem when one phone stops working 109
No power on the G430. 109
CLI is not accessible 110
NVRAM Init 110

Appendix A: Front panel description 113
The front panel of the G430 chassis and EM200 chassis without media modules 113
Media module slots 114
System LEDs 114
USB ports 115
Services port (Services) 115

Compact Flash Interface 115
Contact Closure port (CCA) 116
Implement the Contact Closure feature 116
Router port (ETH WAN) 116
Switch ports (ETH LAN) 116
Reset (RST) and Alternate Software Bank (ASB) buttons. 117
Load firmware from a bank other than the default bank during startup . . 117
The front panel of the Avaya MM710B media module 117
MM710B ports 118
MM710B LEDs 118
The front panel of the Avaya MM711 media module 119
MM711 ports 119
MM711 LEDs 119
The front panel of the Avaya MM712 media module. 120
MM712 ports 120
MM712 LEDs 120
The front panel of the Avaya MM714 media module. 121
MM714 ports 121
MM714 LEDs 121
The front panel of the Avaya MM714B media module 122
MM714B ports 122
MM714B LEDs 122
The front panel of the Avaya MM716 media module. 123
MM716 ports 124
MM716 LEDs 125
The front panel of the Avaya MM717 media module. 125
MM717 ports 126
MM717 LEDs 127
The front panel of the Avaya MM720 media module. 128
MM720 ports 128
MM720 LEDs 128
The front panel of the Avaya MM722 media module. 129
MM722 ports 129
MM722 LEDs 129

Appendix B: Technical specifications 131
G430 Media Gateway specifications 131
EM200 specifications 132
Power cord specifications 133

USB modems supported by the G430 133
USB modems supported by the S8300 133

Appendix C: Running the Avaya Installation Wizard (Avaya IW) 135

Appendix D: Running the Gateway Installation Wizard (GIW) 137
Running the Gateway Installation Wizard (GIW) 137
Performing a basic configuration of the G430 137
Connect a USB modem, if necessary 141
Test the modem connection 142
Testing the modem 142

Appendix E: Power supplies and adjunct systems 143
Typical adjunct power connections 143
Typical adjunct power connections end-to-end 144
Avaya Aura Communication Manager messaging application 145
Call center 145
About Avaya G430 announcement software 145

Appendix F: Information Checklists 147
Installer's Checklist 148
Serial Number and Login Information 149
G430 Serial Number 149
Logins 149
Quick Setup for G430 Media Gateway Processor (MGP) 150
Installation Site Information 151

Appendix G: Equipment List 153

Index 163

About this book

Downloading this book and updates from the Web

You can download the latest version of *Installing and Upgrading the Avaya G430 Media Gateway* from the Avaya Support website. 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 Support website might also contain new product information and updates to the information in this book. You can also download these updates from the Avaya Support website.

Downloading this book

1. Access the Avaya Support website at support.avaya.com
2. Click **Documentation**.
3. Select **Installation, Migrations, Upgrades & Configurations**.
4. Select **G430** under "G".
5. Locate the latest version of the book.
6. Click the book title. Your browser downloads the book.

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. A warning can also indicate the presence of a hazard that could cause personal injury if the hazard is not avoided by following the instructions provided.

DANGER:

A danger statement indicates the presence of a hazard that can result in severe personal injury or death if the hazard is not avoided by following the instructions provided.

ELECTROSTATIC ALERT:

An ESD warning calls attention to situations that can result in ESD damage to electronic components.

SECURITY ALERT:

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

Related resources

For more information on the Avaya G430 Media Gateway and related features, see the following books:

Title	Number
Quick Start for Hardware Installation for the Avaya G430 Media Gateway	03-603236
Overview for the Avaya G430 Media Gateway	03-603235
Administration for the Avaya G430 Media Gateway	03-603228
Avaya G430 CLI Reference	03-603234
Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers	03-300430
Maintenance Commands for Avaya Aura Communication Manager, Media Gateways and Servers	03-300431
Maintenance Procedures for Avaya Aura Communication Manager, Media Gateways and Servers	03-300432

Technical assistance

Avaya provides resources for technical assistance within the US and internationally.

Within the US

- Call the Avaya Technical Consulting Support System at 1-800-225-7585 for help with feature administration and system applications.
- Call the Avaya National Customer Care Support Line at 1-800-242-2121 for help with maintenance and repair.
- Call Avaya Toll Fraud Intervention at 1-800-643-2353 for help with toll fraud.

International

Contact your local Avaya authorized dealer for all international resources.

Trademarks

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

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
- Email, send your comments to:

  document@avaya.com
- Fax, send your comments to:

  1-303-538-1741

Ensure that you mention the name and number of this book, *Installing and Upgrading the Avaya G430 Media Gateway*, 03-603233.

Chapter 1: Before you install

Read this chapter carefully before you begin the installation. If you are installing the G430 at a customer site, read this chapter before going to the customer site.

Before going to site

Before going to the site, it is necessary to read the planning documentation and prepare equipment required for installation.

Preparing required equipment

Make sure you have the necessary equipment to assist you in the installation before you start working.

Equipment required for installation

- One loop start analog trunk for connecting a modem
- A separate telephone line, if needed, for verbal communication during remote configuration

Equipment required for mounting

- A crosspoint screwdriver if rack mounting or wall mounting the G430
- If you will mount the G430 on a flat wall: screws to fasten the G430 to the wall
- If you will mount the G430 on a non-flat wall:
  - A 48 in. x 48 in. (1.2 m x 1.2 m) plytwood board (US: 3/4 inch plywood), 0.75 in. (20 mm) thick.
  - Wood screws to fasten the G430 to the plywood.
  - Screws to fasten the plywood board to the wall (pan head at least ¾ in, #10-12 screw)

Equipment required for installing an S8300 Server

- One USB CD-ROM drive

- A laptop computer with Internet Explorer

Equipment required if you are not installing an S8300 Server

- A PC on the local network, optionally with a USB flash drive
- A laptop computer running Windows XP or Windows 2000 with an Ethernet port recognized by the operating system on the laptop. If the port is recognized, it is listed by the Device Manager.
- A modem to connect to the G430 to enable dial-in configuration. See USB modems supported by the G430 on page 133 for a list of the USB modems supported by the G430.

Obtaining the G430 serial number

Look for the serial number sticker on the back of the G430 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 http://rfa.avaya.com website, this task will require a preliminary trip to the customer site.

Obtaining RFA access

You need to 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
- Associates should point their browsers to the Avaya Associate portal
- Contractors should point their browsers to Avaya.com
- Alternatively go directly to http://rfa.avaya.com

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

Checking license file and Avaya Aura™ Communication Manager versions for a Local Survivable Processor (LSP)

If you are installing an S8300 as a Local Survivable Processor (LSP), the license file for the S8300 must have a Communication Manager release that is equal to or greater than that of the server that acts as primary controller (an S8300, S8400, S87xx, or S85xx). 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 Avaya Aura Communication Manager (CM) that is identical to that of the primary controller.

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

Downloading CM license and authentication files to your laptop

If you are installing a G430 with an S8300 Server as a primary controller, you need license and authentication files for the Communication Manager.

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 http://rfa.avaya.com.
3. Login using your SSO login and password. The AFS and RFA information home page appears.
4. Start the RFA application from the RFA information page. To create and download the license file and authentication file, follow the instructions outlined in the *Avaya Remote Feature Activation (RFA) User Guide*, 03-300149.
5. Use the download or email capabilities of the RFA website to download the license and authentication files to your laptop.

Once the Communication Manager license and authentication files are downloaded to your PC, you can use the Avaya Installation Wizard to install them (see Running the Avaya Installation Wizard (Avaya IW) on page 135. You can also use the Maintenance Web Interface to install the Communication Manager license and authentication files.

Running the Automatic Registration Tool (ART) for the RAS IP address

The ART tool is a software tool that generates a remote access (RAS) IP address and password, for accessing a product attached to a customer's modem. This IP address is required for configuring remote access to a modem on the S8300 or G430. If you need to configure remote access to both the G430 and the S8300, follow this procedure twice, once for the G430 and once for the S8300. For each procedure, a script file is created and downloaded or emailed to you. You can use the installation script to automatically set up an IP address and other alarming parameters.

When you run GIW, you will have the opportunity to import the Electronic Planning Worksheet (EPW). The ART information will be imported along with all the other information in the EPW. Alternatively, if the G430 will be configured using the CLI, keep the installation script to run as a CLI command at the configuration stage.

If the G430 will be configured using Gateway Installation Wizard (GIW) or Avaya Installation Wizard (AIW), and you have an EPW, enter the ART information contained in the installation script into the EPW.

Note:

You must generate and install a License file and Authentication file for the Communication Manager installed on the S8300, before you use the ART tool. Follow the applicable process to register the system in the Automatic Registration Tool (ART). Provision the IP Address for S8300 Remote Access with Configure server by using the **Set Modem Interface** function. Non-Avaya personnel may need to contact their service support or customer care center for IP addresses, depending on entitlements.

Obtaining the RAS IP address and password

1. Access the ART website on your laptop.
2. From the User menu, select **Administer an S8xxx, G430, CCS, CVLAN, or ASG Guard II**.

   The Enter Network Password dialog box appears.
3. Enter your ART user name and password.
4. Click **OK**.

   The **Start of Installation script & IP Addr Admin** screen appears.
5. In the FL Number field, enter the customer's FL number.
6. In the Session Type field, select **Installation Script Administration**.

7. In the Product Type field, select **G430 MEDIA GATEWAY** if you want to configure remote access for the G430, or **S8300 SERVER** if you want to configure remote access for the S8300.
8. In the INADS field, enter the number of the telephone line to which you will connect the modem.
9. Click **Start Installation script & IP Addr Admin**. ART validates your input and the Customer Validation screen appears.
10. Read the customer information displayed, to check that it is correct.
11. In the Customer Type field, select **Other**.
12. Click **Continue Installation Script Administration**. A product list appears.
13. Click the number of the product for which you are configuring remote access. The G430 MEDIA GATEWAY Installation Script Administration Data screen appears.
14. In the Product Name field, enter the product name.
15. In the INADS Number field, make sure the correct customer provided dial-in number for the G430 Media Gateway appears.
16. Click **Continue Installation Script Administration**. ART generates the RAS IP address and password (CHAP secret key) and generates an installation script for the product. Keep the RAS IP address and password to configure your modem later.
17. Click **Download Installation Script File** to download the installation script to your laptop, or **Email Installation Script File** to have the script emailed to you.

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

Downloading recent firmware

Download any recently updated firmware for the G430 and media modules to your laptop. Visit the Avaya Support website to check the latest firmware image file versions against the factory installed versions in the hardware you are installing. Download any firmware image file upgrades you need from the Avaya Support website, and any Communication Manager service packs that may be required for the upgrade.

Obtaining the Electronic Preinstallation Worksheet (EPW)

The EPW is an Excel spreadsheet from which Avaya configuration wizards automatically pull data to configure and install the S8300 Server and the G430 Media Gateway. The EPW is filled in by the customer and project manager, and should be completed before installation.

For greatest efficiency, obtain the Electronic Preinstallation Worksheet (EPW) from the Avaya Support website at http://support.avaya.com/avayaiw.

Site requirements

Inspect the site before you begin the installation. 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.

The G430 may be installed in a 19” rack, mounted on a wall, or placed on a sturdy table. Installation instructions are provided in Installing the Avaya G430 Media Gateway and EM200 on page 25. The ambient temperature should be in the range 32 to 104°F (0-40°C). The humidity should not be higher than 90%.

Environmental verification

Verify that temperatures and clearances are within the recommended technical parameters. Consult the table of Technical Specifications in Technical specifications on page 131.

WARNING:
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 G430 Media Gateway 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 Power cord specifications on page 133.

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 on page 37).

WARNING:

Installation in a Restricted Access Location and secure access are required in Finland, Norway, and Sweden. The G430 Media Gateway relies on two ground connections: first, the mains plugs for the power supplies are required to be connected to AC outlets that have earth contacts; and second, the Supplementary Ground Conductor provided with the system provides a non-removable ground even when the AC cords are disconnected. However, because of unreliable earthing concerns in Finland, Norway, and Sweden, the G430 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 G430 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.

G430 package contents

The G430 chassis and accessories are shipped in a box. The package should contain the following items:

- One Avaya G430 Media Gateway chassis. The required media modules may be installed.
- One accessories box, containing:
  - Two standard mounting brackets
  - One mounting bracket with cable guides
  - Two wall mounting brackets
  - One Supplementary Ground Conductor
  - Nine 4-40 flat head screws
  - Four rubber feet

The Avaya Partner Contact Closure adjunct box, if ordered, is packaged separately.

EM200 package contents

The EM200 chassis and accessories are shipped in a box. If you ordered an EM200 expansion unit or units, each EM200 package should contain the following items:

- One EM200 chassis. The required media modules may be installed.

- One accessories box, containing:
  - One expansion cord
  - Two standard mounting brackets
  - One mounting bracket with cable guides
  - Two wall mounting brackets
  - One Supplementary Ground Conductor
  - Nine 4-40 flat head screws
  - Four rubber feet

Unpacking and checking package contents

For the G430 package and for the EM200 package(s), if ordered:

1. Unpack the G430 and accessories.

   ELECTROSTATIC ALERT:
   Wear an anti-static wrist ground strap whenever handling components of an Avaya G430 Media Gateway or EM200. Connect the strap to an approved ground, such as an unpainted metal surface.

2. Check the contents of the packaging against the customer order.
3. Cross-check the customer 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 also indicated.
4. Verify that all necessary elements have been received and are in good condition. If there are missing or damaged elements, contact your project manager. The planning documentation will list contact information for key personnel.

If you have any questions about the equipment order, or if the equipment has been damaged, contact your project manager.

Chapter 2: Installing the Avaya G430 Media Gateway and EM200

Installing the Avaya G430 Media Gateway consists of installing the G430 chassis, installing the EM200 expansion module(s) if ordered, installing media modules, attaching ground conductors, and connecting the power.

Step 1: Mounting the G430 chassis

You can mount the G430 in a rack, on a wall, or on a table.



ELECTROSTATIC ALERT:

When handling any components of an S8300 Server or G430 Media Gateway, wear an anti-static wrist ground strap. Connect the strap to an approved ground, such as an unpainted metal surface.

Note:

Avaya has developed special hardware platforms for customers with harsh environmental conditions. These platforms have been tested to meet stringent physical and environmental requirements (i.e., shock, vibration, EMI, etc.) imposed by the United States Navy for use on their ships. The platforms make use of specialized racks and reinforcements. If you wish to obtain information about the design and implementation of such a ruggedized solution, contact the Avaya Navy Shipboard Services organization.

Mounting the G430 in a rack

The G430 mounts in a standard 19-inch rack.

You can fasten the G430 to the rack either at the front of the G430 or at the middle. In either case, mounting brackets must be attached to the G430.

There are two types of mounting brackets provided with the G430:

- Without cable guides. Two mounting brackets without cable guides are provided.
- With cable guides. One mounting bracket with cable guides is provided. This bracket provides guides for electrical cables and is useful for cable management.

Brackets without cable guides

Mounting brackets without cable guides can be attached in either of the following positions:

- To each side of the front of the G430 for fastening the chassis to the rack at the front
- To the middle of each side panel of the G430 for fastening the chassis to the rack at the middle

Figure 1: Attaching a mounting bracket to the front of the G430



Figure 2: Attaching a mounting bracket to the middle of the G430



Brackets with cable guides

You can attach the mounting bracket with cable guides to the front of the G430 on one side, as shown in the following figure. If you are fastening the chassis to the rack at the front, use the mounting bracket with cable guides as one of the two front brackets. If you are fastening the chassis to the rack at the middle, use the mounting bracket with cable guides at the front of the chassis, in addition to the two regular mounting brackets on the sides of the chassis. In this case, the mounting bracket with cable guides serves for cable management only — you do not fasten it to the rack.

Note:

It is recommended to attached the mounting bracket with cable guides to the right side of the rack, so as not to block your view of the system LEDs.

Figure 3: Attaching a mounting bracket with cable guides



Attaching each mounting bracket to the G430

The G430 is held in place by mounting screws through the two mounting ears. Fill racks from the bottom; that is, mount units in the lower positions first, to avoid balancing problems and cabling complications.

1. Position a bracket over the desired mounting position.
2. Affix the bracket to the chassis with three of the nine 4-40 flat head screws provided.
3. Tighten with a screwdriver.

Before mounting the G430

- 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 G430 is being mounted in a rack with other equipment already installed, the G430 must be positioned to avoid imbalance.

Note:

The G430 weighs under 11 pounds (5 kg) empty and between 13 and 14 pounds (between 6 and 7 kg) when equipped with media modules.
The EM200 weighs under 11 pounds (5 kg) empty and between 12 and 13 pounds (between 5 and 6 kg) when equipped with media modules.

Mounting the G430 in the rack

1. Position the G430 in the rack. Ensure that there is adequate ventilation.
2. Verify that the screw holes are aligned with the rack hole positions.
3. Insert four rack mounting screws, two on each side.
4. Verify that the G430 is level and horizontal.
5. Tighten the rack mounting screws. Avoid overtightening.

6. Verify that ventilation vents are not obstructed.

Mounting the G430 on a wall

Note:

You can mount a G430 on a wall only if you do not attach any EM200 modules to it.

To mount the G430 on a wall, use the two wall mounting brackets You can also add a mounting bracket with cable guides if desired, as explained in Brackets with cable guides on page 26.

CAUTION:

If you are installing the G430 in the United States of America:

- The AC power supply cord must not be attached to the building wall, for example with wire staples, clamps, and so on.
- You must install the G430 near the AC receptacle (socket outlet) that services the G430.
- You must install the AC power supply cord in a way that minimizes the risk of physical damage to the cord. The cord must not be hanging on the floor, or routed in any way that can subject it to physical abuse.

Attaching brackets to the G430 for wall mounting

Attach a wall mounting bracket to each side of the G430, as shown in Figure 4.

Figure 4: Attaching a bracket to each side of the G430



Fastening the G430 to the wall

Note:

The plywood and the hardware to mount the plywood are customer-provided.

1. If the wall does not have a portion of plywood available, mount a plywood sheet at least ¾ in (2.0 cm) thick and at least 4 x 4 ft (1.2 x 1.2 m) in size, horizontally onto the wall. Make sure the plywood is sufficiently anchored in the wall. Use a minimum of four wood screws and ensure the screws are driven into wall studs, or use four wall anchors rated not less than 50 pounds (22.5 kg) shear strength each.
2. Mark the plywood with the location of the G430 bracket screw holes before fastening the plywood to the wall.
3. Position the G430 so that its front panel is facing up, and secure it to the plywood using a minimum of four screws (pan head at least ¾ in, #10-12 screw).

Placing the G430 on a table

If you install the G430 as a tabletop unit, affix the provided rubber feet to the underside of the G430.

1. Remove the four feet from their packaging.
2. Turn the G430 upside down.
3. Position each foot into one of the mounting sites, near each corner of the chassis.

Step 2: Mounting the EM200 expansion module(s)

You can optionally extend the G430 by attaching one or two EM200 expansion modules to the G430. Since the cables attaching the EM200 expansion modules to the G430 are short, you must install the G430 and EM200s directly above or below each other.

The EM200 expansion modules can be mounted in a rack or on a table, similarly to how the G430 is mounted. Refer to Step 1: Mounting the G430 chassis on page 25. Note that although the figures illustrating the mounting instructions depict a G430, all rack and table mounting procedures apply equally to both the G430 and the EM200. Keep in mind the following:

- If you are mounting the G430 and EM200 module(s) on a table, always place the G430 on top of the EM200(s). This enables easy access in case you need to open the G430 cover in order to add or replace a DSP module or the RAM card.

Note:

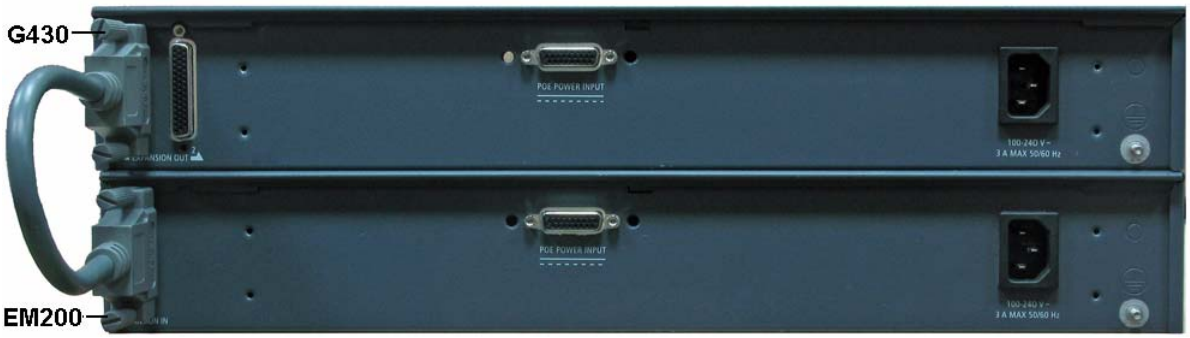
You cannot mount a G430 with EM200 modules on a wall.

Step 3: Connecting EM200 expansion modules to the G430

If you mounted one or two EM200 modules for the purpose of expanding the G430, connect each EM200 to the G430 using the expansion cable supplied with each EM200.

- If you mounted one EM200:
  a. Connect one end of the expansion cable to the CONNECTOR OUT 1 connector on the rear of the G430.
  b. Connect the other end of the expansion cable to the CONNECTOR IN connector on the rear of the EM200.

Figure 5: Connecting an EM200 to the G430



- If you mounted two EM200 modules, connect one EM200 to the CONNECTOR OUT 1 connector on the rear of the G430, and one EM200 to the CONNECTOR OUT 2 connector on the rear of the G430.

Step 4: Installing the media modules

When the G430 chassis and optionally the EM200 module(s) are installed, you can insert the media modules. Each module is shipped with two thumb screws for securing the module in the G430 or EM200 chassis.

Note:

The required media modules are sometimes pre-installed in the G430 or EM200 chassis. If this is the case, skip this step. Read this section only if the media modules are not pre-installed, or if you want to replace modules or add new media modules.

Before inserting media modules into the G430 or EM200 chassis

- Do not install an unsupported combination of media modules. See Combination limitations on page 31.
- Allocate a permissible slot to each media module. See Allocating slots on page 31.

WARNING:

The G430 and EM200 must not be operated with any open slots. Failure to cover empty slots with the supplied blank plates can cause overheating due to inadequate air distribution.

Combination limitations

The G430 chassis is designed to accommodate:

- Up to three of the following telephony media modules: MM710, MM710B, MM711, MM712, MM714, MM714B, MM720, MM722
- Up to two of the following telephony media modules: MM716, MM717
- Up to one S8300 server, in slot V1 only

Each EM200 chassis is designed to accommodate:

- Up to two of the following telephony media modules: MM710, MM170B, MM711, MM712, MM714, MM714B, MM716, MM717, MM720, MM722

Note:

Although you can insert a total of seven MM710 or MM710B media modules in the extended G430 (a G430 with two EM200 expansion modules), the optimum number is four MM710 or MM710B media modules, since the G430 can support up to 100 VoIP channels.

Allocating slots

The G430 chassis has three media module slots, marked V1, V2, and V3 (see Figure 6).Each of the two optional EM200 expansion modules has two media module slots each (see Figure 7). The slots of the EM200 connected to the EXPANSION OUT 1 connector on the rear of the G430 are slots V5 and V6, and the slots of the EM200 connected to the EXPANSION OUT 2 connector on the rear of the G430 are slots V7 and V8. Table 1 lists the permitted slots for each media module.

Allocate a slot for the media module. Make sure your slot allocations allow a permissible slot for every media module.

Figure 6: The G430 front panel ports and slots

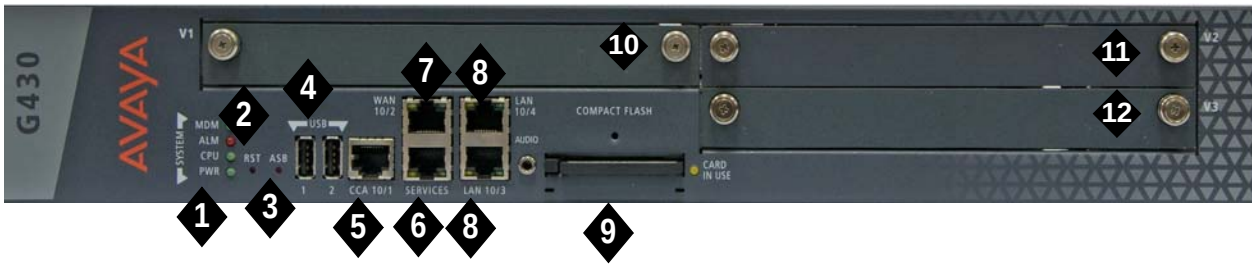


Figure notes:

1. System LEDs
2. RST button
3. ASB button
4. USB 2.0 ports
5. CCA (Contact Closure) port
6. 10/100M Services port
7. 10/100M ETH WAN port
8. 10/100M ETH LAN ports
9. Compact Flash slot
10. V1 — slot for media module or S8300 Server
11. V2 — slot for media module
12. V3 — slot for media module

Figure 7: The EM200 front panel slots



Figure notes:

1. System LEDs
2. V5/V7 — slot for media module
3. V6/V8 — slot for media module

Table 1: Permitted slots for G430 and EM200 media modules

Media module	Permitted slots	Description
MM710	V1-V3, V5-V8	1 T1/E1 ISDN PRI trunk port
MM710B	V1-V3, V5-V8	1 T1/E1 ISDN PRI trunk port
MM711	V1-V3, V5-V8	8 universal analog ports
MM712	V1-V3, V5-V8	8 DCP telephone ports

1 of 2

Table 1: Permitted slots for G430 and EM200 media modules (continued)

Media module	Permitted slots	Description
MM714	V1-V3, V5-V8	4 analog telephone ports and 4 analog trunk ports
MM714B	V1-V3, V5-V8	4 analog telephone ports, 4 analog trunk ports, and an emergency transfer relay
MM716	V1-V3, V5-V8	24 analog ports
MM717	V1-V3, V5-V8	24 DCP telephone ports
MM720	V1-V3, V5-V8	8 ISDN BRI trunk or endpoint (telephone or data) ports
MM722	V1-V3, V5-V8	2 ISDN BRI trunk ports
S8300C or S8300D	V1	CM server

2 of 2

Inserting the S8300 Server

The S8300 can only be inserted in slot V1 on the left side of the G430 Media Gateway.

ELECTROSTATIC ALERT:

Hold media modules only by the edges to avoid damage from static electricity. Do not touch the top or bottom of the circuit board. If possible, wear an anti-static wrist-strap and use an anti-static bag.

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 screwdriver to ensure the captive screws are securely tightened to prevent damage to the equipment.

1. Remove the blank plate from slot V1.
2. Position the server before the V1 bay opening and engage both sides of the module in the interior guides.
3. Slide the S8300 Server slowly into the chassis, maintaining an even pressure to assure that the module does not become twisted or disengaged from the guides.

Figure 8: Inserting the S8300 Server



4. Apply firm pressure to engage the connectors.

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

5. Lock the S8300 Server module into the chassis by tightening the spring-loaded captive screws on the front of the module.

6. After you have inserted the S8300 Server module, if applicable, insert the rest of the media modules. Make sure to insert each module in a permissible slot.

   DANGER:
   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.

Inserting media modules

After you have inserted the S8300 Server module, if applicable, insert the rest of the media modules. Make sure to insert each module in a permissible slot. Remove the blank plate from the empty bay.

ELECTROSTATIC ALERT:

Hold media modules only by the edges to avoid damage from static electricity. Do not touch the top or bottom of the circuit board. If possible, wear a wrist-strap and use an anti-static bag.

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 screwdriver to ensure the captive screws are securely tightened to prevent damage to the equipment.

1. Position the media module before the selected bay on the front of the G430 or EM200 chassis and engage both sides of the module in the interior guides.
2. 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 9: Inserting a media module



3. Apply firm pressure to the front panel of the media module until it is flush with the front panel of the gateway.
4. Tighten each of the spring-loaded captive screws by turning them four times with a screwdriver.

5. Apply firm pressure to the front panel of the media module to ensure full engagement of the connectors.
6. Lock the media module into the chassis by tightening the spring-loaded captive screws on the front of the module.

Tip:

Use the **`show mg list_config`** CLI command to see whether the gateway has identified all the installed media modules correctly. If the gateway does not identify a media module, re-install the media module.

DANGER:

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.

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:
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.

General grounding requirements

Two safety grounds are required to ensure safe operation of each G430 Media Gateway and each EM200: the ground conductor that is part of the AC power cord, and the 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 G430 or EM200, use that cord whenever possible.

Installation location

Select a location for the G430 or EM200 installation that is close enough for use with the supplied secondary grounding conductor. If this location requirement is not met, 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 the length of the supplied secondary grounding conductor from an approved ground, do not install the G430 or EM200 until a licensed electrician is present to install a Supplementary Ground Conductor.

Ground conductor

A 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 G430 or EM200 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).

Ground block

A ground block, supplied by the customer and installed by an electrician, is available for use when you are installing multiple G430 Media Gateways or EM200s . The ground block, intended for rack mounting, has ten terminals available for terminating Supplementary Ground Conductors. Up to ten G430 Media Gateways or EM200s 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.

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.

Restricted Access Location

In Finland, Norway, and Sweden, the G430 Media Gateway and EM200s must be installed in a Restricted Access Location, due to unreliable earthing concerns. 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 G430 or EM200s is gained by the use of a tool (such as a lock and key) or other means of security.

WARNING:
For installations in Finland, Norway, and Sweden, the Avaya G430 Media Gateway and EM200 rely on two ground connections (mains plug with an earth contact, and a Supplementary Ground Conductor).

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.

- 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, or a 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, 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. Must have 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 (26 mm^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.
  - The 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.
  - A 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 G430 and EM200s 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 the G430 or EM200.

DANGER:
Connection of both grounds (through the AC Power Cord and the Supplementary Ground Conductor) is required for safe operation of the G430 or EM200.

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

Attaching the ground wires

Perform the following in each G430 and EM200.

1. Unscrew the lock nut of 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 ground screw.
3. Tightly close the lock nut.

If the ground block has been purchased

1. 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.
2. Attach one end of the remaining 10 AWG (4 mm^2) ground wire to one of the terminals in the ground block and the other end to an approved ground.
3. Cut this ground wire to the length needed to reach the approved ground. Do not coil this wire.

Note:
The ground block is for use with more than one G430 or EM200 in the rack. If the ground block is to be used, you must supply it and have it installed by an electrician.

If the ground block is not being used

1. Attach the Supplementary Ground Conductor to an approved ground.

2. Connect the AC power cable to the inlet receptacle on the rear of the chassis.

Step 7: Connecting power to the EM200 expansion modules

WARNING:
Connect power to the EM200 expansion modules before you connect power to the G430. Failure to do so may cause unexpected results.

For each EM200 module you connected to the G430:

1. Connect the power cable to the power connector on the EM200 back panel.
2. Plug the power cable into a mains socket. The EM200 is now powered.

   The V5-V6 LED on the EM200 front panel lights if the EM200 is connected to the CONNECTOR OUT 1 connector on the rear panel of the G430. This indicates that the two media module slots are considered slot 5 and slot 6 of the G430.

   The V7-V8 LED on the EM200 front panel lights if the EM200 is connected to the CONNECTOR OUT 2 connector on the rear panel of the G430. This indicates that the two media module slots are considered slot 7 and slot 8 of the G430.

   The PWR LED on the front panel lights, indicating the EM200 is powered.

WARNING:
If you wish to move an EM200 in a working system consisting of a G430 and one or two EM200s housing media modules, you must disconnect the EM200 from power before reconnecting the expansion cable to the new location. Failure to do so may cause unexpected results.

Step 6: Connecting power to the G430

After you have mounted the G430, optionally mounted and connected EM200 device(s), installed the media modules, and attached grounding conductors, you can connect power to the G430.

1. Connect the power cable to the power connector on the G430 back panel.

2. Plug the power cable into an AC outlet. The G430 is now powered.

   The PWR LED on the front panel lights. The CPU LED lights up if the firmware is running. At least one LED on each media module, except the S8300, lights up initially and then goes off after about 20 seconds.

Chapter 3: Connecting devices

External endpoint devices can be connected to the ports on the front panels of the installed media modules and to the fixed front panel ports. Before you connect endpoint devices, the G430, and EM200s if desired, should be mounted and all media modules should be inserted.

WARNING:
To reduce the risk of fire, use only 26 AWG or larger telecommunication line cords when installing telephones or adjuncts, or connecting to any media module telecommunication ports.

ATTENTION:
Pour réduire les risques d’incendie, utiliser uniquement des conductors de télécommmunications 26 AWG ou de section supérieure. Pour réduire les risques d'incendie, veuillez n'utiliser que des fils de lignes télécommmunications de 26 AWG ou de section supérieure, lorsque vous connectez des téléphones, des équipements complémentaires, ou pour toute connexion aux ports télécommunications d'une quelconque carte d'équipement.

Step 1: Connecting data and voice devices

There are various possible ways of connecting different devices. See your planning documentation for any topology requirements to connect specific devices to specific ports. As you connect devices, keep a record of the slots and ports into which specific devices are connected. You will need this information when configuring the G430.

Connecting a switch or a network data port

You can connect one or more LAN switches to either of the ETH LAN ports on the front panel.

Connecting a computer to the Services port

A laptop connected directly to the Services port of the G430 requires a specific configuration of its network settings.

Note:

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

1. Set the laptop's TCP/IP properties as follows:
   - IP address: **192.11.13.5**
   - Subnet mask: **255.255.255.252**
   - Disable DNS service
   - Disable WINS Resolution
2. Disable the proxy server in the laptop’s Internet browser settings.
3. Connect the laptop computer to the G430 Services port, using an Ethernet cable.
4. SSH to 192.11.13.6.

To connect the computer to the ETH LAN, port, use a straight network cable with an RJ-45 connector, or a crossover cable with an RJ-45 connector. To connect the computer to the ETH WAN port, use a straight network cable with an RJ-45 connector.

Connecting an IP telephone

Note:

For a full list of supported phones, see Appendix B, *Supported Avaya telephones* in *Overview for the Avaya G430 Media Gateway*, 03-603235.

Connecting the telephone to the G430

1. Wire a telephone to a port on the switch connected to the G430 LAN port. If the switch is a PoE switch, you do not need to plug the IP telephone into a power supply.
2. Plug the telephone into the telephone port.
3. If the IP telephone will be powered independently, plug the IP telephone into a power supply and check that the IP telephone is powered up.

Connecting an ISDN BRI station

Each ISDN port on the MM720 media module 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. However, the MM720 BRI media module supports combining both B-channels together to form a 128-kbps channel. CM 3.1 enables combining B-channels, using BONDing, to form a higher bandwidth connection.
Finally, if the MM720 BRI media module is administered to support BRI stations, it cannot be used as a clock synchronization source.

Connecting one ISDN BRI station to one ISDN port

Connect the station via a standard 8-pin BRI cable to one of the ISDN ports on an MM720 media module.

Connecting 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 10 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 10: RJ-45 splitter wiring for connecting two ISDN BRI stations to one ISDN port

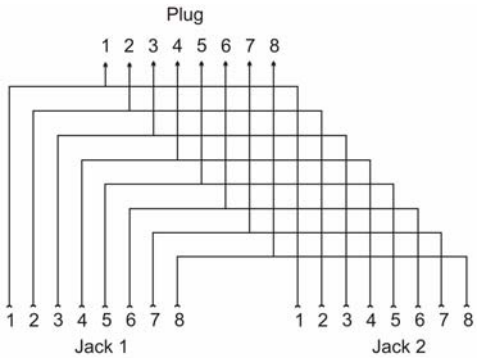
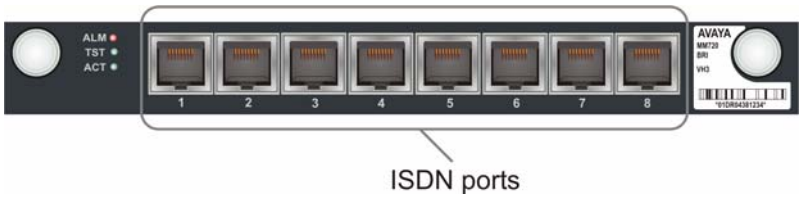


Figure 11: The MM720 media module



Connecting an analog telephone

Note:

For a full list of supported phones, see Appendix B, *Supported Avaya telephones* in *Overview for the Avaya G430 Media Gateway*, 03-603235.

1. Wire a telephone port to one of the following analog ports:
   - A universal analog port on an MM711 media module
   - Any analog line port on a punch down block connected to an MM716 media module. To connect the MM716 media module to a punch down block to enable telephone connection, see Connecting devices to the MM717 and MM716 media modules on page 51.
   - A LINE port on an MM714 or MM714B media module
2. Plug the analog telephone into the telephone port.

Figure 12: The MM711 media module

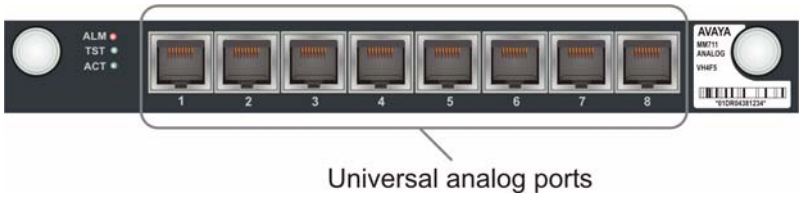


Figure 13: The MM714 media module

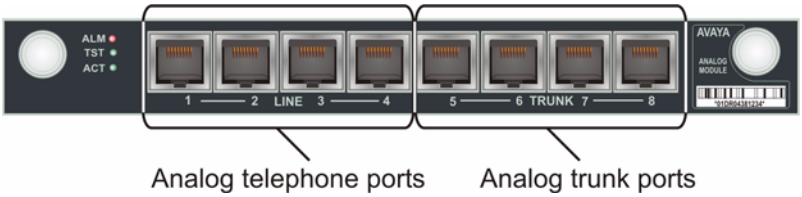


Figure 14: The MM714B media module

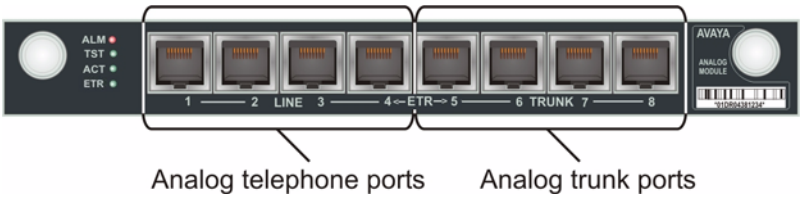
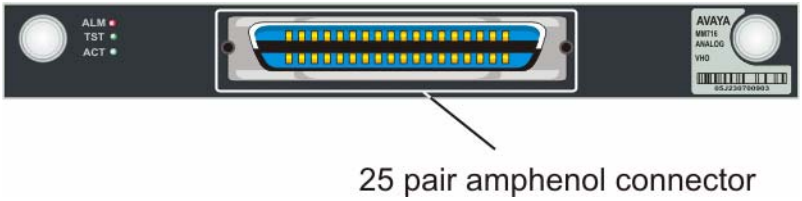


Figure 15: The MM716 media module



Note:

Analog line ports support the following maximum distances:

– For phone equipment with a ringer load below 3 REN: up to 2,000 feet (609.6 m).

Connecting a DCP telephone to an MM712 or MM717 media module

Note:

For a full list of supported phones, see Appendix B, *Supported Avaya telephones* in *Overview for the Avaya G430 Media Gateway*, 03-603235.

1. Wire a telephone port to a DCP port on the G430.

   The following media modules provide DCP telephone ports:

   – MM712. Eight DCP ports

   – MM717. Twenty four DCP ports, provided via a single 25-pair amphenol socket on the front panel. To connect the MM717 media module to a punch down block to enable telephone connection, see Connecting devices to the MM717 and MM716 media modules on page 51.

Figure 16: The MM712 media module

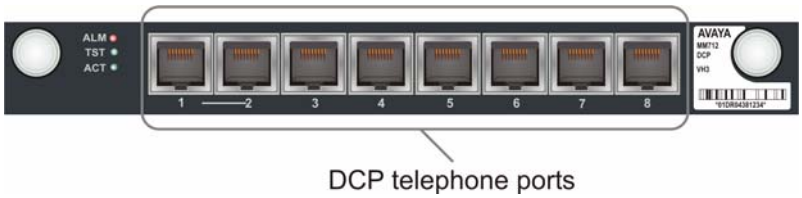
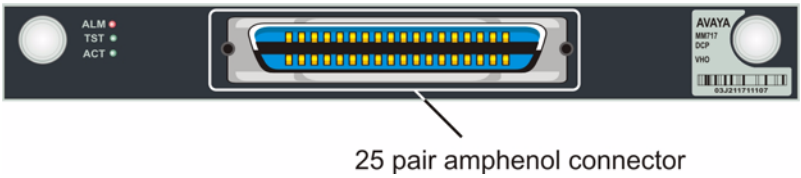


Figure 17: The MM717 media module



2. Plug the DCP telephone into the telephone port.

WARNING:

With the exception of the MM712, all DCP media modules are intended for in-building use only. Phone lines connected to these ports are not to be routed out-of-building. Failure to comply with this could cause harm to personnel and equipment.

Note:

The MM712 and MM717 and media modules support the following maximum loop lengths:
- Up to 5500 ft for 22 AWG wire
- Up to 3500 ft for 24 AWG wire
- Up to 2200 ft for 26 AWG wire

Connecting an analog trunk

Analog trunk

Connect the trunk to one of the following ports:

- Any universal analog port on an MM711 media module
- One of the ports marked TRUNK on an MM714 or MM714B media module

Analog DID trunk

Connect the trunk to one of the following ports:

- Any universal analog port on an MM711 media module
- Any analog line port on a punch down block connected to an MM716 media module. To connect the MM716 media module to a punch down block to enable trunk connection, Connecting devices to the MM717 and MM716 media modules on page 51.
- One of the ports marked Line on an MM714 or MM714B media module

Connecting an E1/T1 trunk

Connect the trunk cable to the E1/T1 port on an MM710 or MM710B media module. The SIG LED lights.

Figure 18: The MM710B media module



Connecting an ISDN BRI trunk

Connect the trunk to any ISDN port on an MM720 or MM722 media module.

Note:

In the US, you need to connect a separately purchased NT1 device to each ISDN port you use to connect an ISDN BRI trunk.

Figure 19: The MM720 media module

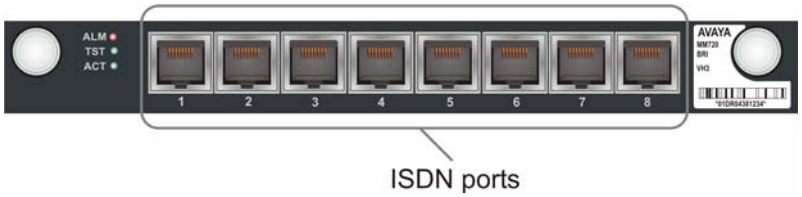
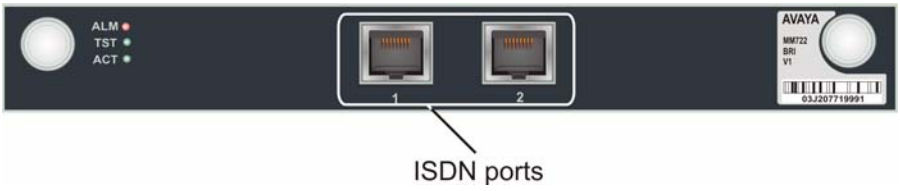


Figure 20: The MM722 media module



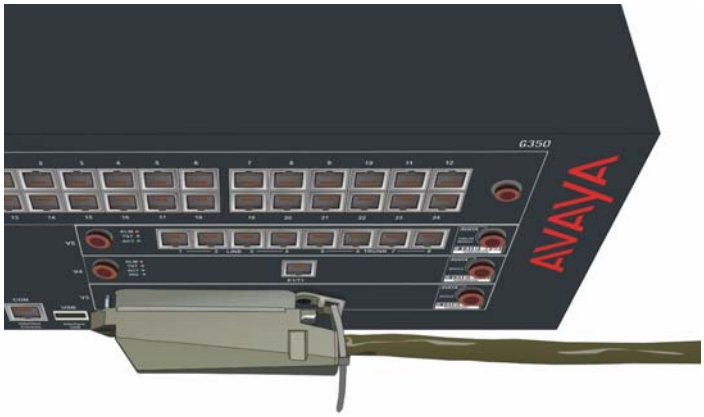
Connecting devices to the MM717 and MM716 media modules

The MM716 and MM717 media modules each have a single 25-pair amphenol socket on the front panel, intended for use with a punch down block. Connect the front panel connector to a punch down block. You can terminate up to 24 endpoint devices on the connected punch down block.

Connecting the MM716 or MM717 front panel connector to a punch down block

1. Connect one end of a CAT5 cable with a 25-pair amphenol connector at each end to the 25-pair socket on the MM716 or MM717 front panel, so that the cable extends to the right of the G430. (The cable you use must be such that the connector you plug into the media module is 90° to the cable.)
2. Tighten the end screw of the amphenol connector to securely fasten the connector to the left side of the front panel socket.
3. Thread a tie wrap through the small bracket to the right of the front panel socket.
4. Fasten the tie wrap around the cable to secure the cable to the right side of the front panel socket.

Figure 21: Attaching and securing the amphenol cable to the MM716 or MM717 25-pair socket



5. Connect the other end of the amphenol cable to a punch down block that converts the single amphenol connector to 24 RJ-11 jacks, as needed. You can now connect endpoint devices to the RJ-11 jacks. For the pin-out of the 25-pair connector, see Table 15.

Step 2: Installing circuit protection

Out-of-building installations of telephones or other standard (tip/ring) devices/terminals that connect to the Avaya G430 Media Gateway media modules require over-voltage and sneak current protection in both buildings. Field installed sneak current protectors must have a maximum current rating 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:

- For the Avaya MM710, MM710B T1/E1. Over-voltage and sneak current protection for the Avaya MM710 is provided on the media module itself.
- For the Avaya MM711, MM714, MM714B, and MM716 Analog. Over-voltage and sneak current protection for these interfaces is provided on the media modules/interfaces. Incoming trunks normally have over-voltage protection provided by the local telephone company. Analog voice terminals use one of the following types of combined over-voltage and sneak current protection at both building entry points:
  - Gas tube with heat coil. 4B1E-W
  - Solid state with heat coil. 4C1S
  - IROB. 146C (4-lines) or 146F (25-lines)
- For the Avaya MM712 DCP: either 146E IROB (In-Range Out-of-Building) or 4C3S-75 solid state protectors for over-voltage and sneak current.
- For the Avaya MM722 ISDN-BRI: over-voltage and sneak current protection are provided on the media modules themselves.
- For the Avaya MM720 ISDN-BRI: network-side applications require an NT-1 device. Tie trunk applications require either the 146E IROB (In-Range Out-of-Building) or 4C3S-75 solid state protectors for over-voltage and sneak current.

WARNING:
Only service-trained personnel are to install these circuit protection devices.

WARNING:
With the exception of the MM712, all DCP media modules are intended for in-building use only. Phone lines connected to these ports are not to be routed out-of-building. Failure to comply with this could cause harm to personnel and equipment.

Step 3: Connecting to the Wide Area Network (WAN)

Since the G430 contains an internal router, you can connect the G430 directly to a WAN endpoint device. You can also connect a WAN endpoint device to the G430 via an external router.

Connecting an Ethernet WAN link

You must connect the Ethernet WAN line (DSL, firewall, etc.) to the Ethernet WAN port on the front panel of the Avaya G430 Media Gateway chassis. This port is marked ETH WAN. See Figure 6. Use a CAT5 Ethernet cable to connect the WAN line to the port.

Connecting an external router to the G430

You can connect a router to any of the following ports on the G430:

- The ETH WAN port on the G430 front panel
- The ETH LAN ports on the G430 front panel

Step 4: 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.

Installing the CBC

Before you begin, be sure the telephone lines are cross-connected to the appropriate media module(s).

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 in (30.5 cm) away from exposed telephone cables whenever possible.

Step 5: Installing the Avaya Partner Contact Closure Adjunct

The Contact Closure feature is a controllable relay providing dry contacts for various applications. To implement the contact closure feature, you connect an Avaya Partner Contact Closure Adjunct box to the CCA port on the G430 chassis. The adjunct box provides two contact closures that can be operated in either a “normally closed” or “normally open” state. The contact closures can control auxiliary devices such as devices that automatically lock or unlock doors or voice recording units. The CCA port can be configured so that the connected devices can be controlled by an end device, such as a telephone. For example, a user can unlock a door by keying a sequence into a telephone keypad.

Installing the contact closure

1. Follow the installation instructions in the *Avaya Partner Contact Closure Adjunct Installation Instructions* leaflet to install the Contact Closure and connect the auxiliary devices that will be activated and deactivated by the Contact Closure relays.
2. Note which device is connected to each relay. You will need this information for configuration.
3. Connect the Avaya Partner Contact Closure adjunct box to the CC port on the G430 front panel. Use a 24 gauge minimum telephone wire, no longer than 200 ft, with a standard four wire RJ-11 connector.

Chapter 4: Connecting and enabling a USB modem for remote access

You can connect a USB modem to the G430 to enable configuration from a remote location.

If an S8300 is installed in the G430, leave a modem connected permanently to enable reporting of alarms to remote locations.

Note:

If you choose to configure the G430 by running an installation wizard, you can enable a modem with the wizard as part of the configuration. Instructions for connecting the modem are included in Appendix C: Running the Avaya Installation Wizard (Avaya IW) on page 135 and in Appendix D: Running the Gateway Installation Wizard (GIW) on page 127. You do not need to read this chapter.

Note:

If you run GIW, ensure that services can log in to the system using USB modem after you run the GIW.

Connecting and enabling a USB modem (G430 without S8300)

You can enable a USB modem on a USB port on the G430 front panel. See USB modems supported by the G430 on page 133 for a list of the USB modems supported by the G430

Note:

No configuration is necessary for Services personnel to remotely access the gateway through a USB modem.

1. Prepare a PC with a CD-ROM drive, SSH client software, and a TFTP server on the network. This may be needed for installing software and firmware upgrades.

   Note:

   Firmware upgrades for the G430 and media modules can either be installed from CD or downloaded from the Web.

2. Download GIW (Gateway Installation Wizard) from the Avaya Support website (support.avaya.com/avaygiw) to the laptop computer. The laptop should be running Windows 2000, or Windows XP to support GIW.

3. Set the laptop's TCP/IP properties as follows:
   - IP address: 192.11.13.5
   - Subnet mask: 255.255.255.252
   - Disable DNS service
   - Disable WINS Resolution
4. Disable the proxy server in the laptop’s Internet browser settings.
5. Connect an Ethernet cable from the laptop computer to the G430 Services port.
6. From your laptop computer, double-click the GIW icon to run GIW. The Overview screen appears.
7. Click **Continue**. The Gateway Connection Details screen appears.
8. Choose **Select if this is a G430 Gateway**.
9. Enter your Username and Password.
10. Click **Continue** until the Modem Type Selection screen appears.
11. Select **USB Modem**.
12. Click **Continue**. The G430 USB Modem Configuration screen appears.
13. In the PPP IP Address field, enter the RAS IP address of the modem obtained using the ART tool. See Running the Automatic Registration Tool (ART) for the RAS IP address on page 20.
14. Enter the PPP Subnet Mask.
15. Select the authentication method:
    - If you have an Avaya Service contract, check **Enable ASG Authentication** to enable remote access to the device.
    - If you do not have an Avaya Service contract:
      - Check **Enable CHAP Authentication**.
      - In the **CHAP Secret** field, enter the CHAP secret key obtained using the ART tool. See Running the Automatic Registration Tool (ART) for the RAS IP address on page 20.
      - In the **Confirm CHAP Secret** field, re-enter the CHAP secret key.
16. Click **Continue** until you exit the Gateway Installation Wizard.
17. Click **Finish**.
18. Connect a USB modem to a working telephone line.
19. Connect one end of a USB cable to the modem.
20. Connect the other end of the USB cable to a USB port on the G430 front panel.

Testing the modem connection (G430 without S8300)

Dial into the modem to verify that you can authenticate to the modem.

1. Setup a dialup connection on a remote PC with the following settings:
   - Automatically detect settings.
   - No Username, Password, or Domain.
   - Security > Show Terminal Window.
2. Dial in to the modem from the remote PC.
3. When prompted, provide the rasaccess login and password in the Terminal Window.
4. Close the Terminal Window to complete the connection.
5. Activate an SSH session.
6. Login valid authentication to the G430 CLI.

Connecting and enabling a USB modem (G430 with S8300)

You can connect a USB modem to a USB port on the S8300 front panel. See USB modems supported by the S8300 on page 133 for a list of the USB modems supported by the S8300.

Maintenance web pages

Most of the preparations you are making require you to access the Maintenance web pages part of Avaya Integrated Management (AIM) from your laptop. After accessing the Maintenance web pages, leave the Maintenance web pages open until you have completed all the preparations.

Changing the modem settings on the Configure Server Maintenance Web Page

1. Select **Configure Server** from the left-hand menu on the Maintenance web page. The Back Up Data page appears.
2. Follow the on-screen instructions to back up the current data.
3. Click **Continue**.
4. Select **Configure individual services**.
5. Click **Continue**.

6. From the left navigation menu, click **Set Modem Interface**. The Set Modem Interface page appears.
7. Enter the RAS IP address you obtained using the ART tool. See Running the Automatic Registration Tool (ART) for the RAS IP address on page 20.
8. Click **Change modem settings**.
9. Click **Continue**.
10. Click **Close Window**.

Note:

You can only change the modem settings on the Configure Server Maintenance Web Pages if you have an Avaya Maintenance contract.

Connecting and enabling a USB modem (G430 with S8300)

If your installation includes an S8300 Server module, you must connect the USB modem to the S8300. After the G430 is configured, you can leave the modem permanently connected to enable the S8300 to report alarms to remote locations.

Note:

If you require a USB CD-ROM drive to download software upgrades, connect the USB CD-ROM drive to the remaining available USB port on the S8300 Server.

Connecting and enabling the modem

1. Connect the USB modem to a working telephone line.
2. Connect the modem to one of the USB ports on the S8300 Server.
3. From the navigation menu of the Maintenance Web Pages, select **Security > Modem**. The Modem page appears.

Figure 22: Modem page



4. Select **Enable modem for unlimited incoming calls**.
5. Click **Submit**.

Testing the modem connection (G430 with S8300)

1. Setup a dialup connection on a remote PC with the following settings:
   - Automatically detect settings.
   - No Username, Password, or Domain.
   - Security > Show Terminal Window.
2. Dial in to the modem from the remote PC.
3. When prompted, provide the rasaccess login and password in the Terminal Window.
4. Close the Terminal Window to complete the connection.
5. Activate an SSH session.
6. Login valid authentication to the Linux CLI.

If a USB CD-ROM drive is required to download software upgrades

Connect the USB CD-ROM drive to the remaining available USB port on the S8300 Server.

Chapter 5: Configuring the G430

The G430 requires software configuration. The G430 can be configured using:

- The Avaya Installation Wizard (Avaya IW). Avaya IW is a wizard that prompts you for all configurations required to complete the installation of the G430. Avaya IW is used only to configure a G430 with an S8300. See Appendix C: Running the Avaya Installation Wizard (Avaya IW) on page 135.
- The Gateway Installation Wizard (GIW). The GIW is a wizard that prompts you for all configurations required to complete the installation of the G430. You can run GIW to configure a G430 without an S8300. See Appendix D: Running the Gateway Installation Wizard (GIW) on page 127.
- The Avaya G430 Command Line Interface (CLI). The CLI is a comprehensive tool for configuring the gateway and includes all supported configuration tasks. For information about configuration using the CLI, see *Administration for the Avaya G430 Media Gateway*, 03-603228. For detailed information on CLI commands, see the *Avaya G430 CLI Reference*, 03-603234.

The G430 can be accessed:

- At the customer site via a laptop connected to the Services port of the G430. For information about connecting a laptop to the Services port, see Connecting a computer to the Services port on page 43.
- From a remote location via a modem. For information about connecting and enabling a modem, see Chapter 4: Connecting and enabling a USB modem for remote access on page 55.
- Remotely through the network. For information about preparing a newly installed G430 for configuration via the network, see Configuring basic gateway connectivity on page 61.

Configuring basic gateway connectivity

You can run an installation script on a newly installed gateway to configure the basic network parameters required to achieve network connectivity. A remote technician can then further configure the gateway as required. Note that the installation script does not require running any CLI command.

Note:

The installation script is supported from branch gateway firmware version 29.22.x.

1. Prepare a laptop with SSH client software.

2. Set the laptop's TCP/IP properties as follows:
   - IP address: 192.11.13.5
   - Subnet mask: 255.255.255.252
   - Disable DNS service
   - Disable WINS Resolution
3. Connect the laptop computer to the G430 Services port, using an Ethernet cable.
4. SSH to 192.11.13.6.
5. At the prompt, enter username **root** and password **root**.
6. At the prompt, configure a new password.
7. At the prompt, enter **y** to configure basic gateway connectivity.

   Note:

   If you enter **n** but then change your mind, you can use the **`script-config`** CLI command to run the installation script, so long as you have not saved any configuration changes you may have made.
8. You are prompted to configure the following parameters. For each parameter, you can enter a value, or press Enter to accept the default value shown in square brackets:
   - VLAN number
   - IP address for the primary management interface
   - Subnet mask for the primary management interface
   - IP address for the default gateway (router)
   - Up to four IP addresses to specify the Media Gateway Controllers
   - Hostname for the G430

The settings you configured are displayed, and you are prompted for confirmation.

- If you confirm the settings, they are saved and the G430 reboots.
- If you do not confirm the settings, you are prompted to re-configure them. If you enter **y**, the parameters are presented again for configuration.

9. Connect the Ethernet port to the network to enable remote access to the gateway. A remote technician can now further configure the gateway using the CLI.

Chapter 6: After installation

After initial configuration, it is necessary to test the installation, and remove the installation equipment.

Step 1: Testing the installation

When the installation is complete, simple tests must be performed to test telephone and data connectivity.

Testing data connectivity

Test data connectivity by pinging the IP address of each device to test the device's connectivity within the network and outside the network.

Testing telephones

1. Make outgoing calls from the telephone. Make sure you hear a dial tone when you pick up the receiver. Make sure you can make both an internal (within the local network) and an external (outside the local network) call.
2. Make a call to the telephone from both within the network and outside of the network.

Testing trunks

Use the facility test call feature to verify that each trunk is functioning properly.

For information about how to use the facility test call feature, see *Maintenance Procedures for Avaya Aura Communication Manager, Media Gateways and Server*s, 03-300432.

LSP failover testing

If you have an S8300 Server installed in the G430 and configured as an LSP, you need to perform a test to make sure that the LSP takes over control of the G430 if the G430 becomes disconnected from the primary MGCs (Media Gateway Controller).

Note:

If SLS mode is enabled and the primary controller and LSP both fail, then the G430 enters SLS mode.

1. Verify that valid translations are file synchronized to the LSP by logging into Avaya Aura Communication Manager from the LSP and listing either stations or trunks, see *Administering Avaya Aura™ Communication Manager*, 03-300509. Verify that the list of stations or trunks is valid. If the files are not synchronized, verify that you have correctly configured the required IP address(es) for the primary controller(s) (MGC). If you are using Avaya IW to configure the G430, the following are key actions that must be done in the wizard to ensure correct IP address configuration:

   a. In the Usage options screen, select the one of the following usage options that corresponds to the correct primary controller type:

      - **Install an LSP that is associated with an S8500 Primary Controller**.
      - **Install an LSP that is associated with an S8300 Primary Controller**.

      If you selected the correct usage option, the Primary Controller IP Address screen appears later in the wizard, and calls for the required primary controller IP addresses for your primary controller type. The following IP addresses need to be configured for each primary controller type:

Primary media gateway controller	Number of IP addresses to be configured	IP addresses to configure
S8300X	1	The IP address of the primary S8300X
S85XX	2	The IP address of the S85XX's Control-LAN card (CLAN) and the IP address of the S8500

   b. In the Primary Controller IP address screen, enter all the required IP addresses for the primary controller type.

      There may be a delay after running AIW until the LSP is registered with the primary MGC and the translations are file synchronized.

Note:

You must add the LSP server correctly to the Main CM Server.

2. If valid translations are not file synchronized to the LSP, do the following:
   a. From a SAT session run from the primary controller, verify that the LSP node-name and IP address are correctly entered.
   b. Use the **`save translation lsp`** command to start the file synchronization process.
   c. Log in again to Avaya Aura Communication Manager from the LSP and list either stations or trunks.
   d. Verify that the list of stations or trunks is valid.
3. Disconnect the G430 from the primary controller, ensuring that all telephones are still connected or have network connectivity to the G430.
4. Verify that calls can be made between local telephones using the locally connected outside lines to the G430.

Note:

See also "Auto Fallback for H.248 Gateways" in *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504 and the Migrate H.248 MG to primary" screen command in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Table 2: IP addresses and controllers

Primary media gateway controller	IP addresses to configure
S8300	The IP address of the primary S8300
S8400	The IP address of the S8400's C-LAN or the IP address of an Ethernet port on the S8400 configured for processor Ethernet connections
S8500	The IP address of the S8500's C-LAN or the IP address of an Ethernet port on the S8500 configured for processor Ethernet connections
S8510	The IP address of the S8510's C-LAN or the IP address of an Ethernet port on the S8510 configured for processor Ethernet connections
S8710	The IP address of the S8710's C-LAN and the IP address of alternate C-LAN boards connected to the S8710
S8720	The IP address of the S8720's C-LAN and the IP address of alternate C-LAN boards connected to the S8720
S8730	The IP address of the S8730's C-LAN and the IP address of alternate C-LAN boards connected to the S8730

Step 2: Removing the installation equipment

Remove all equipment that you used to assist you in the installation process. This may include the CD-ROM drive, the software upgrade CDs, the laptop computer, and the modem (for installations without an S8300X module only).

Note:

If you have an S8300X Server module installed in the G430, leave the modem connected to enable reporting of alarms to remote locations.

Chapter 7: Adding media modules and devices

When adding new devices to the G430, consult your project manager for topology requirements for specific ports to be connected to specific devices.

Adding a media module

Various media modules can be added to the Avaya G430 Media Gateway.

Adding voice modules

You can hot-swap voice modules. This means that you can add or remove a voice module in the Avaya G430 Media Gateway or EM200 while the system is running, without any disruption to your network. Configuration of the G430 is not necessary when you add or remove a voice module. Configuration is only necessary when you add telephones, fax machines, and trunks to the new module. See Adding a telephone on page 67 and Adding a trunk on page 68.

Some configuration of the Avaya Aura Communication Manager is necessary when you install an MM710, MM710B, MM720, or MM722 media module. See *Administrator's Guide for Avaya Aura Communication Manager*, 555-233-506. Also, for an MM710, MM720, or MM722, it is usually advisable to set the media module as the synchronization source of the G430. For information about setting the synchronization source of the G430, see the *AvayaG430CLI Reference*, 03-603234.

Adding a telephone

You must connect, configure and test the telephone before adding the telephone to the Avaya G430 Media Gateway.

Connecting the telephone

To connect a new telephone, see the following sections:

- Connecting an IP telephone on page 44
- Connecting an analog telephone on page 46
- Connecting a DCP telephone to an MM712 or MM717 media module on page 48

Configuring the telephone on the Communication Manager

- Standalone: Configuration may be performed on site by connecting a laptop computer to the Services port of the G430 or S8300, or remotely via a modem connected to the G430 or S8300, or remotely over the network.
- LSP: Configuration is done on the primary CM server.

For information about connecting a laptop to the Services port, see Connecting a computer to the Services port on page 43. For information about preparing a modem, see Chapter 4: Connecting and enabling a USB modem for remote access on page 55. For information about configuration, see Chapter 5: Configuring the G430 on page 61.

Recording telephone information for software configuration

When you add a new telephone - IP, DCP or Analog - note the following information for software configuration:

- Name and location of the owner of the telephone
- Model number of the telephone
- Extension of the telephone
- Slot and port number on the Avaya G430 Media Gateway to which the telephone connects (this does not apply to IP telephones).

Testing the telephone

1. Make outgoing calls from the telephone. Make sure you hear a dial tone when you pick up the receiver. Make sure you can make both an internal (within the local network) and an external (outside of the local network) call.
2. Make a call to the telephone from both within the network and outside of the network.

Adding a trunk

You must order, connect, configure, and test the trunk before adding the trunk to the Avaya G430 Media Gateway.

Ordering the trunk

- Make sure that the telephone service provider installs the trunk near the physical location of the G430 and verifies that the trunk is working properly before you contact the technician who is performing or supervising the configuration
- Note the telephone number of the trunk

Special considerations when ordering an analog trunk

When you order an analog trunk, there are several recommendations depending on your system's particular needs:

- For optimal functioning of the MM714B Emergency Transfer Relay feature, it is recommended to use a loop-start trunk
- For access to voice mail systems in the United States, it is recommended to use a ground start trunk to ensure that calls are properly disconnected when the outside caller disconnects.
  - Ground start trunks may be provided via the MM711, MM714B or MM714 media modules.

Note:

If you use the MM714B with ground start, you must use a ground start button for ETR.

- Request conditioned lines to ensure satisfactory voice quality and trunking interactions

Connecting the trunk

To connect a new trunk, see one of the following sections:

- Connecting an analog trunk on page 49
- Connecting an E1/T1 trunk on page 50
- Connecting an ISDN BRI trunk on page 50

Configuring the trunk on CM

- Standalone: Configuration may be performed on site by connecting a laptop computer to the Services port of the G430 or S8300, or remotely via a modem connected to the G430 or S8300, or remotely over the network.
- LSP: Configuration is done on the primary CM server.

Note:

Sync timing configuration for a T1/E1 trunk is done via the CLI.

For information about connecting a laptop to the Services port, see Connecting a computer to the Services port on page 43. For information about preparing a modem, see Chapter 4: Connecting and enabling a USB modem for remote access on page 55. For information about configuration, see Chapter 5: Configuring the G430 on page 61.

Recording trunk information for software configuration

When you add a new trunk, note the following information for software configuration:

- Slot and port number on the Avaya G430 Media Gateway or EM200 to which the trunk connects
- Telephone number of the trunk

Testing the trunk

1. Make outgoing calls from the trunk. Ask the technician that is performing or supervising the configuration for instructions how to access the trunk. Make sure you can make both an internal (within the local network) and an external (outside of the local network) call.
2. Make a call into the G430 trunk.

Adding a Broadband Line (xDSL or cable modem)

You must order, connect, configure and test the Broadband line before adding the line to the Avaya G430 Media Gateway.

Ordering the Broadband line

If you need to order the Broadband line, make sure that the service provider installs the line near the physical location of the G430 and verifies that the line is working before you configure the WAN on the G430.

Connecting the Broadband line

To connect a Broadband line, see Step 3: Connecting to the Wide Area Network (WAN) on page 53.

Configuring the Broadband line on the G430

Configuration may be performed on site by connecting a laptop computer to the Services port of the G430, or remotely via a modem connected to the G430 or S8300, or remotely over the network.

For information about connecting a laptop to the Services port, see Connecting a computer to the Services port on page 43. For information about preparing a modem, see Chapter 4: Connecting and enabling a USB modem for remote access on page 55. For information about configuration, see Chapter 5: Configuring the G430 on page 61.

Testing the Broadband link

After installation of the Broadband line is complete, test the link by pinging the gateway WAN FastEthernet IP address, and performing a trace route test in order to test connectivity with the network and outside the network.

Adding an Avaya Partner Contact Closure Adjunct

To install an Avaya Partner Contact Closure Adjunct, follow the instructions in Step 5: Installing the Avaya Partner Contact Closure Adjunct on page 54.

Chapter 8: Upgrading and replacing Field Replaceable Units

You can add or replace a VoIP module, as well as add or remove components of the upgrade memory kit. Refer to **Equipment List** on page 153 for ordering information.

Inserting or removing an MP10, MP20 or MP80 VoIP module

The G430 has one on-board VoIP module providing 25 VoIP channels for G.711 and G.726 and 20 channels for G.729, and an additional slot for the optional insertion of an MP10, MP20, or MP80 VoIP module.

The field replaceable VoIP module slot is located on the G430 main board. You must remove the G430 cover to insert or remove a VoIP module.

This procedure requires the following steps:

1. Removing the G430 cover
2. Inserting a VoIP module
3. Removing a VoIP module — Skip this step if you are inserting a module into an empty slot.
4. Replacing the G430 cover

Removing the G430 cover



VOLTAGE ALERT:
Disconnect the G430 from the external power source before proceeding.



ELECTROSTATIC ALERT:
Do not touch any components on the printed circuit board.

1. Disconnect the G430 power cable from the mains power supply.
2. Disconnect all cables (data and power) connected to the G430 and its media modules, both front and rear. Note to which connector each cable is connected, so that you can reconnect them correctly.

3. Remove the G430 from the rack or wall, if it is wall or rack mounted.
4. If mounting brackets are attached to the G430, remove them.
5. Unscrew the 8 cover screws, indicated by small arrows etched into the cover:
   - Remove one screw from the top (see Figure 23).
   - Remove four screws from the right side (see Figure 24).
   - Remove three screws from the left side (see Figure 25).
6. Lift the cover off the G430.

Figure 23: Removing the G430 cover screw from the top of the device



Figure notes:

1. G430 top cover screw

Figure 24: Removing G430 cover screws from the right side



Figure notes:

1. – 4. Four G430 right-side cover screws

Figure 25: Removing G430 cover screws from the left side



Figure notes:

1. – 3. Three G430 left-side cover screws

Inserting a VoIP module

ELECTROSTATIC ALERT:
Hold modules only by the edges to avoid damage from static electricity. Do not touch the top or bottom of the circuit board. If possible, wear a wrist-strap and use an anti-static bag.

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

1. Locate the VoIP module slot (see Figure 26).
2. Position the VoIP module at a 45 degree angle to the main board, and start inserting it into the VoIP module slot (see Figure 26).

Figure 26: Inserting a VoIP module into the VoIP module slot

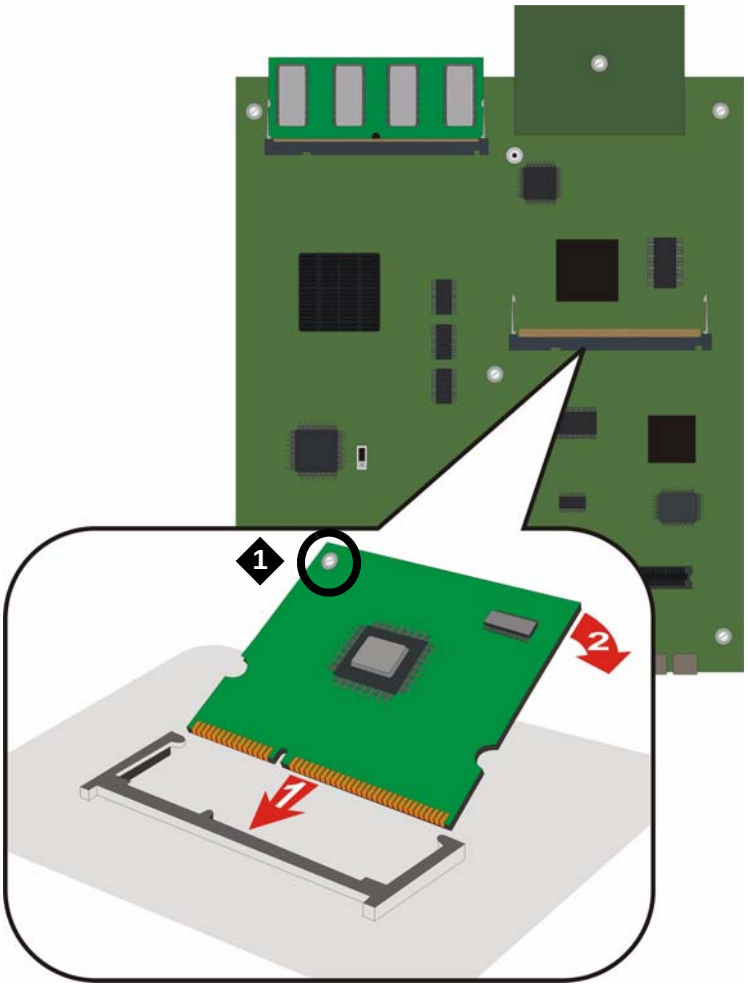


Figure notes:

1. VoIP module locking screw

3. Push the module in all the way. Do not use too much force.
4. Flatten the module so it is flush with the main board. The latches at both sides click shut.
5. Tighten the locking screw affixed to the VoIP module. This secures the VoIP module to the motherboard.

Removing a VoIP module

ELECTROSTATIC ALERT:
Hold modules only by the edges to avoid damage from static electricity. Do not touch the top or bottom of the circuit board. If possible, wear a wrist-strap and use an anti-static bag.

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

1. Locate the VoIP module slot (see Figure 26).
2. Unscrew the locking screw attaching the VoIP module to the motherboard (see Figure 26).
3. Open the latches on both sides of the module slot. The module lifts up.
4. Pull out the module. Hold the module only at the edges.

Replacing the G430 cover

ELECTROSTATIC ALERT:
Do not touch any components on the printed circuit board.

1. Place the G430 cover back on the unit.
2. Screw in the 8 cover screws you previously removed. Their locations are indicated by small arrows etched into the cover:
   - One screw on the top (see Figure 23).
   - Four screws on the right side (see Figure 24).
   - Three screws on the left side (see Figure 25).
3. Attach the mounting brackets to the G430, if applicable.
4. Replace the G430 in the rack or mount on the wall, if applicable.
5. Re-connect all cables (data and power) that you disconnected from the G430 and its media modules, both front and rear.
6. Connect the G430 power cable into a mains socket.

7. Use the **show platform mainboard** CLI command to make sure the G430 is working properly. For example, when the G430 is working properly, output includes:

```
MAINBOARD BOARD
---------------
Type                    : G430
Description             : Avaya Inc., G430 Media Gateway
Serial Number           : 08IS26191007
HW Vintage              : 4
HW Suffix               : F
FW Version              : 29.18.0
No Fault Messages       : No Fault Messages
```

When a VoIP module is successfully installed in the optional VoIP module slot, output for the slot includes:

```
MEDIA SOCKET #2
------------------
Type                    : MP80 VoIP DSP Module
Description             : VoIP DSP resource with 80 channels
Serial Number           : 07IS15812717
HW Vintage              : 0
HW Suffix               : B
Faults                  : No Fault Messages
```

When no VoIP module is installed in the optional VoIP module slot, the output for the slot includes:

```
MEDIA SOCKET #2
------------------
Type                    : UNKNOWN
Description             : UNKNOWN
Serial Number           : UNKNOWN
HW Vintage              : UNKNOWN
HW Suffix               : UNKNOWN
Faults                  : NOT PRESENT
```

Installing the upgrade memory kit

The upgrade memory kit enables increasing the number of announcement files on the G430 from 256 to 1024, by storing them on a removable compact flash. This also increases the total amount of announcement time from 45 minutes to four hours. However, since the announcements are played from RAM, you must also increase RAM to 512 MB.

The upgrade memory kit contains:

- 1 GB compact flash memory card
- Two RAM memory cards. For the G430, use the 512 MB RAM card.

This section describes the steps required to install or remove the upgrade memory kit components in the Avaya G430:

- Replacing a RAM card
- Inserting or removing a compact flash memory card

Replacing a RAM card

The G430 has a single RAM slot housing a 256 MB RAM card. If you wish to support an increased number of announcement files, you must upgrade the G430 memory by replacing the 256 MB RAM card with a 512 MB RAM card.

The RAM slot is located on the G430 main board. You must remove the G430 cover to replace a RAM card. This procedure includes the following steps:

1. Removing the G430 cover.
2. Replacing the RAM card.
3. Replacing the G430 cover.

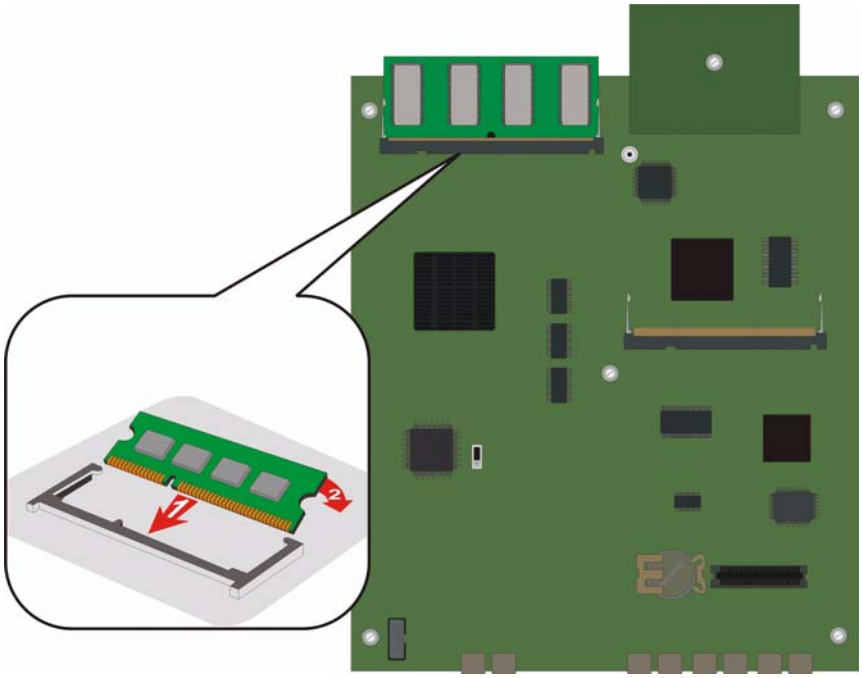
Replacing the RAM card

ELECTROSTATIC ALERT:
Hold the module only by its edges to avoid damage from static electricity. Do not touch the top or bottom of the circuit board. If possible, wear a wrist-strap and use an anti-static bag.

1. Locate the RAM slot (see Figure 27).
2. Open the latches on both sides of the RAM slot. The RAM card lifts up.
3. Pull out the 256 RAM card.

4. Insert the 512 RAM card provided in the kit into the RAM slot, and push in all the way. Do not use too much force.
5. Flatten the RAM card so it is flush with the main board. The latches at both sides click shut.

Figure 27: Replacing the RAM card



Inserting or removing a compact flash memory card

The G430 supports hot insertion and removal of a compact flash memory card without power drop, provided the compact flash is not in use when it is removed.

Inserting a compact flash memory card

1. Remove the blank plate covering the compact flash memory card slot, located in the center of the main board.
2. Position the compact flash memory card so that the vendor name is facing up and the connector is pointing toward the G430, and gently insert it into the compact flash slot.
3. After installing the compact flash memory card and the additional 256 MB RAM card, the announcement files are not automatically moved from the internal flash to the compact flash. To move them:

a. Make sure the gateway is registered to CM.

b. At the CM, set **enable CF** to **y** in the **change media-gateway** screen.

c. In the SAT interface of the CM, enter **`enable announcement-board`**.

The announcement files are copied from internal flash to the compact flash, and the yellow CARD IN USE LED associated with the compact flash flashes.

4. Use the **`show platform mainboard`** G430 CLI command to make sure the G430 is working properly and to check the status of the compact flash and RAM memory. For example:

```
MAINBOARD BOARD
------------------
Type                    : G430
Description             : Avaya Inc., G430 Media Gateway
Serial Number           : 08IS26191007
HW Vintage              : 4
HW Suffix               : F
FW Version              : 29.18.0
No Fault Messages       : No Fault Messages

RAM MEMORY SOCKET #1
------------------
Type                    : 512MB DDR SDRAM memory module
Serial Number           : 0b2c7605
Manufacture Part Num    : 64A6M64M8L-A06EWQU
Faults                  : No Fault Messages

COMPACT FLASH MEMORY
--------------------
Type                    : 2.0 GB
Serial Number           : STI1M2a407200161753
Model Number            : STI Flash 8.0.0
Faults                  : OK
```

Removing a compact flash memory card

After installing a compact flash memory card, you may decide to remove it for one of several reasons. The following sections provide instructions for safe removal of a compact flash memory card in each possible scenario.

- Replacing a compact flash memory card with a different compact flash memory card holding a different set of announcements
- Replacing a compact flash memory card while retaining the current announcements. You may wish to do this because the current compact flash memory card failed, or you want to have two copies of the announcement files, or you want to use a faster compact flash card.
- Downgrading from a compact flash to internal flash memory

Replacing a compact flash memory card with a different compact flash memory card

1. At the SAT interface of the CM, enter **`disable announcement-board`**.

   Important:
   If you do not enter the SAT command **`disable announcement-board`**, then, when you insert the new compact flash, its contents will be overwritten by the contents of the old compact flash.

2. Make sure the yellow CARD IN USE LED associated with the compact flash is not flashing.

   Important:
   If a compact flash is removed while it is in use, the announcement files on the compact flash may become corrupted and the G430 may reset, causing all announcement files in RAM to be lost.

3. Remove the compact flash memory card.
4. Insert the new compact flash memory card into the compact flash slot.
5. At the SAT interface of the CM, enter **`enable announcement-board`**.

Replacing a compact flash memory card while retaining the current announcements

1. Make sure the yellow CARD IN USE LED associated with the compact flash is not flashing.

   Important:
   If a compact flash is removed while it is in use, the announcement files on the compact flash may become corrupted and the G430 may reset, causing all announcement files in RAM to be lost.

2. Remove the compact flash memory card.
3. Insert the new compact flash memory card into the compact flash slot.

   The announcement files of the old compact flash are written to the new compact flash.

Downgrading from a compact flash to internal flash memory

You can downgrade from using up to 1024 announcements on a compact flash to using up to 256 announcements on the internal flash.

Important:
The internal flash can only store up to 256 announcement files, totaling no more than 45 minutes.

1. Backup the announcements from the compact flash to a USB device by entering the G430 command **backup config usb *usb-device backup-name* announcements-compact-flash**.

   Note:

   If you have only a few announcement files, you can use the G430 command **copy announcement-file usb** to copy them one by one.

2. At the SAT interface of the CM, enter **disable announcement-board**, and then set **enable CF** to **n** in the **change media-gateway** screen.
3. Make sure the yellow CARD IN USE LED associated with the compact flash is not flashing.

   Important:

   If a compact flash is removed while it is in use, the announcement files on the compact flash may become corrupted and the G430 may reset, causing all announcement files in RAM to be lost.

4. Remove the compact flash memory card.
5. Optionally replace the 512 MB RAM card with the 256 MB RAM card (see Replacing a RAM card).
6. At the SAT interface of the CM, enter **enable announcement-board**.
7. Make sure there are no more than 256 announcement files in the backup. If the number of announcement files exceeds 256, manually delete as many as necessary in the backup directory.
8. Restore the announcements from the USB device to internal flash by entering the G430 command **restore usb *usb-device backup-name* announcements-internal-flash**.

   Note:

   If you copied the announcement files one by one, you can restore them one by one using the G430 command **copy ftp announcement-file**.

9. Screw on the blank plate to cover the compact flash slot.

Chapter 9: Upgrading the G430 firmware

Software used to control the Avaya G430 Media Gateway itself and media modules installed on the G430 is called firmware. You can upgrade the firmware on the Avaya G430 Media Gateway and media modules using various different tools, each suitable for specific types of installation.

Upgrading G430 firmware using Avaya Software Update Manager

You can use Avaya Software Update Manager to view your network inventory and the firmware vintages of devices on your network. Avaya Software Update Manager can also check the software versions currently in use against the latest versions available from Avaya and recommend updates when a newer version is available. Based on this information, you can download new firmware to multiple network devices simultaneously from a single management station, ensuring all devices are updated.

You can use Avaya Software Update Manager to take a new release from Avaya's website and store it on your hard disk for subsequent downloading to the appropriate devices.

Avaya Software Update Manager is a server application hosted on the Avaya Network Management server. The server stores all the software retrieved from the Web and can download the software to appropriate devices. You may also copy files containing embedded software to the server. You can reach the server locally or via remote access, so you can update the software on your devices from anywhere in the world.

Avaya Software Update Manager is part of the Integrated Management Enterprise Package which is an entitlement for all Avaya Aura Communication Manager non-introductory offers.

For information about using Avaya Software Update Manager, see the *Avaya Integrated Management Software Update Manager User Guide*, 14-300168.

Upgrading G430 firmware from the primary controller

For a G430 without an S8300 or for a G430 with an S8300 installed as an LSP, you can upgrade G430 firmware from the remotely located primary controller. The primary controller may be an S8300, S85XX, S87XX, or S88XX server. See the guide for the primary controller for information about upgrading firmware from the primary controller. See *Upgrading, Migrating, and Converting Avaya Servers and Gateways*, 03-300412.

Note:

You can only upgrade using FTP on the S85XX, S87XX, and S88XX servers.

Upgrading G430 firmware using Gateway Installation Wizard (GIW)

1. Prepare installation worksheets. See Preparing installation worksheets on page 89.
2. Download GIW from the Avaya Support website (support.avaya.com/avayagiw) to the laptop computer. The laptop should be running Windows 2000, or Windows XP to support GIW.
3. Set up a TFTP server on the G430 network. See Setting up a TFTP server on page 91. The GIW runs the CLI commands on the G430 so the G430 can obtain the files from the TFTP server.
4. Download the G430 firmware files to the TFTP server. See Downloading G430 firmware files to a local TFTP server on page 91.
5. Run GIW to perform the upgrade. For instructions on performing the upgrade, see Appendix D: Running the Gateway Installation Wizard (GIW) on page 127.

Note:

This upgrade must be done locally.

Note:

You can only use GIW to upgrade firmware on a G430 that does not contain an S8300.

Upgrading G430 firmware using Avaya Installation Wizard (IW)

For a G430 with an S8300C/D installed, you can use Avaya IW to upgrade G430 firmware. You can run Avaya IW from a remote location if the software is loaded locally. You can point your browser to the IP address of the S8300C/D if you are in the customer network or via the modem connection.

Note:

To upgrade the Avaya CM software use the Software Upgrade Manager (see the *Avaya Software Update Manager User Guide*, 14-300168).

1. Prepare installation worksheets. See Preparing installation worksheets on page 89.
2. Place the upgrade software and firmware files on a laptop. These files are on the Avaya Aura Communication Manager CD-ROM. To upgrade the G430 firmware, insert the Communication Manager CD-ROM into a CD-ROM drive connected to a laptop. Alternatively, you can upload the individual files to the hard drive of the laptop. For more details, see *Job Aid: Avaya Installation Wizard*, 555-245-754.

   Note:

   The CD-ROM may not contain the latest firmware. Check the Avaya Support website for the latest firmware versions and compare these with the versions in the directory. If the CD-ROM does not contain the latest versions, download the latest versions from the Avaya Support website to the laptop.
3. Connect the laptop to the services port of the S8300 Server.
4. Access Avaya IW. See *Job Aid: Avaya Installation Wizard*, 555-245-754.

Upgrading G430 firmware using the CLI via FTP/TFTP

You can upgrade firmware via FTP/TFTP using the CLI. You can perform the upgrade remotely via a modem connection, but the upgrade files must first be downloaded to an FTP or TFTP server on the LAN connected to the G430.

1. Prepare installation worksheets. See Preparing installation worksheets on page 89.
2. Set up an FTP or TFTP server on the LAN connected to the G430. For information about setting up a TFTP server, see Setting up a TFTP server on page 91.

   Note:

   If you use an FTP server, the G430 prompts you for a username and password when you enter a command to transfer a file. Also, when opening an FTP connection to the S8300, all anonymous FTP file transfers are restricted to the /var/home/ftp/pub directory. Permission for anonymous FTP users to create files in other directories is denied.
   You must enable the S8300 FTP server from the Maintenance web page. The S8300 FTP server disables itself after 15 minutes.
3. Download the firmware files to the FTP or TFTP server. See Downloading G430 firmware files to a local TFTP server on page 91 or Installing firmware from the TFTP server on the S8300 Server on page 92.
4. Connect to the G430 via modem or via the Services port on the front panel. For information about connecting the G430 to the Services port, see Connecting a computer to the Services port on page 43. For information about connecting and enabling a modem for remote access, see Chapter 4: Connecting and enabling a USB modem for remote access on page 55.
5. Run CLI commands. See CLI commands for upgrading G430 firmware via FTP/TFTP on page 88.

CLI commands for upgrading G430 firmware via FTP/TFTP

You can use CLI commands to upload an upgrade file to the G430. For each of these commands, include the full path of the file and the IP address of the FTP or TFTP host as parameters. You must use the specific path to the file on the FTP or TFTP server according to the home directory of the service (FTP or TFTP) that you are using. When you enter the command, the CLI prompts you for a username and password.

- Use the **`copy ftp EW_archive`** command to upgrade the Java applet for Avaya G430 Manager software from an FTP server
- Use the **`copy ftp module`** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from an FTP server

- Use the **copy ftp SW_imageA** command to upgrade the G430 firmware into Bank A from an FTP server
- Use the **copy ftp SW_imageB** command to upgrade the G430 firmware into Bank B from an FTP server
- Use the **copy tftp EW_archive** command to upgrade the Java applet for Avaya G430 Manager software from a TFTP server
- Use the **copy tftp module** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from a TFTP server
- Use the **copy tftp SW_imageA** command to upgrade the G430 firmware into Bank A from a TFTP server
- Use the **copy tftp SW_imageB** command to upgrade the G430 firmware into Bank B from a TFTP server

Example upgrade via FTP/TFTP using the CLI

To upgrade the firmware of an MM712 media module in slot 3 from a TFTP server with the IP address *192.1.1.10*, where the home directory is *c:\home\ftp* and the upgrade file is located in the directory *c:\home\ftp\version*, use the following command:

```
copy tftp module \version\mm712v51.fdl 192.1.1.10 3
```

Note:

When uploading firmware from the S8300, use only the file name, without the directory path, in the command line. Otherwise, the procedure will fail. For instance, in the example above, you must use the following command:
`copy tftp module mm712v51.fdl 192.1.1.10 3`

Note:

When uploading firmware from the S8300 using TFTP, you may need to enable TFTP service in the Set LAN Security parameters of your web server.

The following example uploads a firmware version with the path and file name *C:\g430.net* from an FTP server with the IP address *149.49.134.153* to Bank A of the G430:

```
copy ftp SW_imageA C:\g430.net 149.49.134.153
```

Preparing installation worksheets

Before you perform the upgrade, you must enter the names of the target software and firmware versions that you need to install in the software and firmware upgrade worksheet. If you will need to set up a TFTP server, you also need to plan the TFTP server IP address, login, and password.

Entering values in Server Values worksheet

Enter software and firmware upgrade file names in the following table:

Table 3: Software and firmware upgrade file names

Items for Upgrading	New file name for target
File for LSP and primary controller (not used with Gateway Installation Wizard or for individual files)	
G430 Processor	
G430 Device Manager	
MM710 E1/T1 media module	
MM710B E1/T1 media module	
MM711 Analog Port/Trunk media module	
MM712 DCP media module	
MM714 Analog Port/Trunk media module	
MM714B Analog Port/Trunk media module	
MM716 Analog Port/Trunk media module	
MM717 24-port DCP media module	
MM720 BRI media module	
MM722 BRI Trunk media module	

Enter the TFTP server information in the following table:

Table 4: Global Settings for TFTP Server

TFTP Server IP Address	TFTP Server Directory

Setting up a TFTP server

To load individual firmware files on an Avaya G430 Media Gateway, you must place the files on a PC connected to the customer's LAN or on an S8300 Server in the customer's network. Later, you will log onto the G430 and use its TFTP capability to download the new firmware. If you can use an S8300 Server to stage the firmware, see Installing firmware from the TFTP server on the S8300 Server on page 92. If not, a TFTP server must be set up on the LAN.

Note:

A Linux or Unix TFTP server should be used only if a Linux or Unix TFTP server already exists on the local network. In this case, download the appropriate files to your laptop and give it to the customer for proper placement and execution.

Downloading G430 firmware files to a local TFTP server

1. Access the www.avaya.com/support website.
2. Navigate to G430 Media Gateway downloads.
3. Locate the file names that match the files listed in your installation worksheet. See Table 5 for sample firmware file names.
4. Double-click the file name of the file you want to download. A File Download window appears.

   Note:

   Downloading files can occasionally add a [1] to the file name. Rename the file if necessary.

5. Select **Save this file to disk**.
6. Save the file to directory on the TFTP server on the local LAN that was created for this purpose. See Setting up a TFTP server on page 91.

   Note:

   If you are performing the upgrade using the G430's Command Line Interface (CLI), you can place the upgrade files on an FTP server. However, the GIW requires that the files be placed on a TFTP server.

Table 5: Sample Software and Firmware File names

Component	File name Example
G430 Processors	
G430 Processor	*g430_sw_21_11_0.bin*
G430 Device Manager	*g430_emweb_1_0_7.bin*
media modules	
MM710 E1/T1 media module	*mm710v3.fdl*
MM710B E1/T1 media module	*mm710bv47.fdl*
MM711 Analog Port/Trunk media module (version 6 or earlier)	*mm711v16.fdl*
MM711 Analog Port/Trunk media module (version 7)	*mm711h7v21.fdl*
MM711 Analog Port/Trunk media module (version 20 or later)	*mm711h20v54.fdl*
MM712 DCP media module	*mm712v14.fdl*
MM714 Analog Port/Trunk media module	*mm714v5.fdl*
MM714B Analog Port/Trunk media module	*mm714h10v93.fdl*
MM716 Analog Port/Trunk media module	*mm716v80.fdl*
MM717 DCP media module	*mm717v3.fdl*
MM720 BRI media module	*mm720v1.fdl*
MM722 BRI media module	*mm722v3.fdl*

Installing firmware from the TFTP server on the S8300 Server

Instead of using a separately configured TFTP server on the LAN, you can use the TFTP server capability of an S8300 Server to stage the firmware for upgrading the G430. To do this, you must copy the individual firmware files to the */var/home/ftp/pub* directory on the S8300 Server using the Download Files web page on the S8300 Server. You must then copy the files to the */tftpboot* directory of the S8300 Server.

After copying the files to the */tftpboot* directory, you can use the GIW to install the files to the G430 or its media modules by specifying the S8300 Server's IP address as the TFTP server containing the new firmware files.

Note:

You only have to do this if you have not upgraded the S8300 first or if you did upgrade it first and found that the gateway files on the Communication Manager CD were out of date. Otherwise, when you upgrade the S8300, the files appear in the */tftpboot* directory automatically.

Copying firmware files to the */tftpboot* directory of an S8300 Server

1. Use ssh craft@<ip address> to access the S8300 Server command line.
2. Address the password/challenge as required for access.
3. At the Linux prompt, type **`cd /var/home/ftp/pub`** and press **<Enter>**. The Linux prompt reappears. The current directory has changed to */var/home/ftp/pub*.
4. At the Linux prompt, type **`mv`** <***`firmware_filename`***> **`/tftpboot`**, and press **<Enter>** to move the firmware file to the */tftpboot* directory. To move multiple firmware files (most firmware files have an .bin suffix; the media module firmware files have a .fdl suffix), use the command **`mv *.bin /tftpboot`** or **`mv *.fdl /tftpboot`**. The Linux prompt reappears. The firmware file has been moved to the */tftpboot* directory. If you copy the firmware using the cp command, remove the files from the */var/home/ftp/pub* directory after you have copied them.
5. Repeat step 4, if necessary, for each firmware file you want to install.
6. At the Linux prompt, type **`cd /tftpboot`**. The Linux prompt reappears. The current directory has changed to */tftpboot*.
7. At the Linux prompt, type **`ls`**, and press **<Enter>**. A list of files in the directory appears.
8. Check the directory to make sure the firmware files you want to install are listed.

Upgrading G430 firmware using the CLI via a USB device

You can upgrade firmware via a USB mass storage device using the CLI. The upgrade files must first be downloaded to a local PC.

1. Prepare installation worksheets. See Preparing installation worksheets on page 89.
2. Download the firmware files to a PC. See Downloading G430 firmware files to a local PC on page 94.
3. Insert a USB mass storage device into the PC's USB port, and copy the firmware files to the USB mass storage device.

4. Remove the USB mass storage device from the PC, and insert it into a G430 USB port.
5. Run CLI commands to copy the firmware files from the USB mass storage device to the G430. See CLI Commands for upgrading G430 firmware via a USB device on page 94.

CLI Commands for upgrading G430 firmware via a USB device

You can use CLI commands to upload an upgrade file from a USB mass storage device to the G430. You must use the specific path to the file on the USB mass storage device.

- Use the **`copy usb EW_archive`** command to upgrade the Java applet for Avaya G430 Manager software from a USB mass storage device
- Use the **`copy usb module`** command, followed by the slot number of the module you want to upgrade, to upgrade the firmware on a media module from a USB mass storage device
- Use the **`copy usb SW_imageA`** command to upgrade the G430 firmware into Bank A from a USB mass storage device
- Use the **`copy usb SW_imageB`** command to upgrade the G430 firmware into Bank B from a USB mass storage device

Example upgrade using the CLI via a USB device

To upgrade the firmware of an MM712 media module in slot 3 from a USB mass storage device where the upgrade file is located in the directory *temp*\, use the following command:

```
copy usb module usb-device0 \temp\mm712v51.fdl 3
```

Downloading G430 firmware files to a local PC

1. Access the www.avaya.com/support website.
2. Navigate to G430 Media Gateway downloads.
3. Locate the file names that match the files listed in your installation worksheet. See Table 5 for sample firmware file names.
4. Double-click the file name of the file you want to download. A File Download window appears.
5. Select **Save this file to disk**.
6. Save the file to a directory on the local PC.

Note:

Use WinZip or another zip file tool to unzip the file, if necessary, *before* you copy the file to the PC.

Chapter 10: Upgrading IP phone configuration and firmware files

The Avaya G430 Media Gateway supports Trivial File Transfer Protocol (TFTP) downloading of configuration files and firmware files for IP phones. TFTP can be used to download image files, upgrade scripts, and settings files to IP phones. The local TFTP server stores the files and supports requests to read files from the its outgoing directory for phone images and scripts.

You can use CLI procedures for downloading the files for IP phone upgrade from the G430 TFTP server.

Note:

You can also upgrade IP phones using the S8300. For more details, see *Downloading Avaya 46xx IP Telephone Software Using Avaya Media Servers*.

IP telephones supported by the local TFTP Server feature

- **H.323**:
  - 4601
  - 4601+
  - 4602
  - 4602SW
  - 4602SW+
  - 4606
  - 4610SW
  - 4612/24
  - 4620
  - 4620SW
  - 4621SW
  - 4622SW
  - 4690

- **SIP**:
  - SIP phone: 4602 SIP
  - 4602SW
  - 4602SW+
  - 4610SW
  - 4620SW
  - 4621SW

IP telephones not supported by the local TFTP Server feature

- 4630
- 4630SW

Note:

If you have an S8300 installed in the G430, you can alternatively upgrade IP phones using the CM web pages.

Note:

You can also upgrade IP phones using Avaya IW or GIW, as described in Appendix C: Running the Avaya Installation Wizard (Avaya IW) on page 135 and Appendix D: Running the Gateway Installation Wizard (GIW) on page 127.

Note:

An alternative tool, the Avaya Software Update Manager (4.0 or higher), is a GUI application that greatly simplifies the IP phone upgrade process, avoiding the need to know the file names of the necessary upgrade files for each IP phone type. For further information, see *Avaya Software Update Manager User Guide*, 14-300168.

Note:

The IP address of the TFTP server is the PMI.

Administering the upgrade

When using supported IP phones with the G430, the IP phones require the downloading of the settings file and the upgrade scripts. These files are stored in the script banks in NVRAM and are preserved in the event of a reset or power failure. There are two script banks.

In addition, each phone can have a booter application and a phone application. There are four banks that can store up to two phone images (booter and phone application files) at any given time. Since the image files are stored in RAM, a reset or power failure *erases* these files. The image files are used only for upgrading the IP phone, so there is no need to store them permanently. However, the scripts are used by the IP phones when they are reset, and are therefore stored in NVRAM. You can upgrade up to two types of phones and then release the banks for use with another IP phone type.

There are cases where the image files are the same for different IP phone types. In these cases, you can download the image files once for the IP phones that use the same image. The scripts are global to all the supported IP phone images.

You can download and then upload setting script files in order to update their content. It is not recommended to change the upgrade script.

By default, the RAM allocation for TFTP server is 10 MB. You can increase the RAM allocation for TFTP server to up to 11.264 MB at the expense of the Sniffer cache application. The maximum RAM for both applications is 12 MB.

There are four image banks, supporting two IP phone images in RAM, provided the combined file sizes do not exceed the RAM allocation for TFTP server. The maximum size for a booter application or phone application file is 4.5 MB. Thus, it is possible that in some cases, the allocation may only suffice for one complete IP phone image and not two.

CAUTION:

To activate a change in RAM allocation to the TFTP server, reset is required. Upon reset, any phone image files stored in RAM are erased.

Note:

Previous releases of TFTP server required the configuration of the DHCP server option 43/176 with the named value pair TFTPDIR=/phonedir/ in order to allow the IP phone to access the files in this directory. This configuration is still supported but is no longer required.

Upgrading the IP telephone

IP phone upgrade files include script files, boot images files, and phone application image files. You can download these files to a remote FTP/TFTP/SCP server, or you can download them to a laptop and copy them to a USB device. You can then copy the upgrade files to the G430.

Note:

An SCP server can be used for copying the script files, which do not exceed 128 KB, but cannot be used for copying image files.
You cannot use SCP to copy 46xxsettings files as they exceed 128 KB.

Note:

The G430 uses the SSH protocol to support the use of SCP for secure file transfer. When using SCP, the G430 is the SCP client, and an SCP server must be configured on the management station. For more information about establishing an SCP session, see *Administration for the Avaya G430 Media Gateway*, 03-603228.

1. Check the available memory size for the image files using the **`show application-memory`** command. If the memory size needs to be changed, proceed to step 2, otherwise proceed to step 6.
2. Set the memory size for the image files using the **`ip tftp-server file-system size`** command.
3. Copy the running configuration to the start-up configuration using the **`copy running-config startup-config`** command.
4. Reset the G430 using the **`reset`** command.
5. From the Avaya Support website, obtain the desired phone upgrade files (script files, boot image files, phone application image files), using either of the following methods:
   - Download the phone upgrade files to a remote FTP/TFTP/SCP server. Note that SCP can be used to download script files but not image files.
   - Download the upgrade files to a laptop and copy them to a USB mass storage device.
6. Copy the script files for the IP phone family.
   - To copy from the remote FTP/SCP/TFTP server, use one of the following commands:
     - **`copy scp phone-script`**
     - **`copy ftp phone-script`**
     - **`copy tftp phone-script`**
   - To copy from the USB device, insert the USB device into a G430 USB port and copy the files to the resident TFTP server using the **`copy usb phone-script`** command.
7. Copy the boot image files for up to two IP phone types.
   - To copy from the remote FTP/TFTP server, use either the **`copy ftp phone-image`** command or the **`copy tftp phone-image`** command for each IP phone type.
   - To copy from the USB device, insert the USB device into a G430 USB port and copy the files to the resident TFTP server using the **`copy usb phone-image`** command.
8. Copy the phone application image files for up to two IP phone types.
   - To copy from the remote FTP/TFTP server, use either the **`copy ftp phone-image`** command or the **`copy tftp phone-image`** command for each IP phone type.
   - To copy from the USB device, insert the USB device into a G430 USB port and copy the files to the resident TFTP server using the **`copy usb phone-image`** command.
9. Reset the phones and wait for the installation to be completed.

Note:

Once the upgrade procedure is complete, you can delete the files using the **erase phone-image** command.

TFTP IP telephone upgrade examples

In the following example, 4602SW and 4602D phones, which use the same image files, are upgraded first. Later, 4620 phones are upgraded. The script files are not copied for the second upgrade, since they are already stored in NVRAM.

Upgrading the 4602SW and 4602D phones

1. Check the available memory size for the image files using the **show application-memory** command. If the memory size is smaller than the combined sizes of the image files for the phones, proceed to step 2, otherwise proceed to step 5.
2. Set the memory size for the image files using the **ip tftp-server file-system size** command. For example:

```
G430-001(super)# ip tftp-server file-system-size 12228
To change ip tftp-server file system size, copy the running configuration
to the start-up configuration file, and reset the device
G430-001(super)
```

3. Copy the running configuration to the start-up configuration using the **copy running-config startup-config** command. For example:

```
G430-001(super)# copy running-config startup-config
Beginning copy operation ..................... Done!
```

4. Reset the G430 using the **reset** command. For example:

```
G430-001(super)# reset
This command will reset the device
*** Reset the device *** - do you want to continue (Y/N)? y

Resetting the device...
```

5. From the Avaya Support website, download the desired phone upgrade files (script files, boot image files, phone application image files) to a remote FTP server at IP address 192.168.49.10.

6. Copy the script files for the 46xx IP phone family using the **copy ftp phone-script** command. For example:

```
G430-001(super)# copy ftp phone-scriptA 46xxupgrade.txt 192.168.49.10
Confirmation - do you want to continue (Y/N)? y

Username: root
Password:
Beginning download operation ...

This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-script-file status'
command
G430-001(super)#
G430-001(super)# copy ftp phone-scriptB 46xxupgrade.txt 192.168.49.10
Confirmation - do you want to continue (Y/N)? y

Username: root
Password:
Beginning download operation ...

This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-script-file status'
command
G430-001(super)#
```

7. Copy the boot image files for the Avaya 4602 IP telephone using the **copy ftp phone-image** command. For example:

```
G430-001(super)# copy ftp phone-imageA pub\4602dbte1_8.bin 192.168.49.10

Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
G430-001(super)# copy ftp phone-imageB pub\4602sbte1_8.bin 192.168.49.10

Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
```

8. Copy the phone application image files for the 4602 IP phone type DEF4602D using the **copy ftp phone-image** command. For example:

```
G430-001(super)# copy ftp phone-imageC pub\4602dape_8.bin 192.168.49.10

Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
G430-001(super)# copy ftp phone-imageD pub\4602sape_8.bin 192.168.49.10

Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
```

9. Reset the phones and wait for the installation to be completed.

Upgrading 4620 IP phones

1. Copy the boot image files for the 4620 IP phone using the **copy ftp phone-image** command. For example:

```
G430-001(super)# copy ftp phone-imageA pub\bbla20_1817.bin 192.168.49.10


Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
```

2. Copy the phone application image files for the 4620 IP phone using the **copy ftp phone-image** command. For example:

```
G430-001(super)# copy ftp phone-imageB pub\def20r1_8_1.bin 192.168.49.10

Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
```

Note:

Once the upgrade procedure is complete, you can delete the files using the **erase phone-image** command.

Failure scenarios and repair actions

There are various configuration related problems which will cause the upgrade to fail. The scenarios can be repaired by readjusting the downloading or configuration settings.

Table 6: Failure scenarios and repair actions

Problem	Possible cause	Action
"Free Application Memory is xxx MB. Use **show application-memory** for more details"	You tried to configure more memory than is available in the main bank.	Re-adjust the allocation of memory between the Sniffer cache application and the TFTP server. Be sure the Sniffer allocation is not needed for trouble shooting.
"Application Memory reached its limits. Sniffer and TFTP server application memory sizes restore to defaults"	You tried to download configuration files after configuring the total memory allocations for applications and Sniffer to more than 12 Mb in the startup configuration and performing a reset.	None. The memory allocations are set to the default values.
Cannot download file to Gateway		See the specific error message you receive.

1 of 2

Table 6: Failure scenarios and repair actions (continued)

Problem	Possible cause	Action
"Not enough memory in RAM"	The remote file is larger than the available RAM.	Free more space in the RAM using the **`erase phone-script`** or **`erase phone-image`** command.
"Not enough memory in NVRAM"	The remote file is larger than the available NVRAM.	Free space in the NVRAM using the **`erase phone-script`** command.
"File already Exists in other Bank"	You tried to download the same file to more than one bank.	None. You cannot load two files with the same file name to more than one bank.
“TFTP - General failure”	File name or path incorrect	Check the file name and path.
“Can't start upload operation. Wrong operation parameters or other operation already in progress, please try again”	You are trying to upload a file from an empty bank.	Upload from a different bank. Download a file to the bank.
		2 of 2

Upgrading considerations

- Configuration files, such as upgrade script and setting files, are copied to the phone configuration banks in NVRAM, while phone images are stored in RAM

  Note:

  Image files are cleared if you reset the gateway.

- Phone image banks are stored in the same TFTP directory. Therefore, you cannot copy the same file name to more then one bank. Copying a file to a bank containing a file with the same file name causes the old file to be overwritten by the new one.
- File names for IP phone image files and script files are limited to 32 characters

Chapter 11: Backing up and restoring the G430

You can backup and restore the G430 to and from a USB mass storage device using a single CLI command for backup and a single CLI command for restore. This is especially helpful for efficient restoring or replicating of a G430 media gateway.

If the G430 is located remotely, you can backup and restore the G430 files one by one, using TFTP/FTP/SCP servers.

For information about G430 backup and restore, see chapter 5 in *Administration for the Avaya G430 Media Gateway*, 03-603228.

Chapter 12: Troubleshooting

You can have problems with phones, a trunk, the power, or the . It is necessary to identify the specific problem to figure out how it can be resolved. In addition, you may have to perform an NVRAM initialization if you are unable to access the CLI.

One telephone stops working

If one telephone in the network stops working, but the other telephones and data devices continue to work normally, the problem is probably with the telephone itself. There could also be a problem with the telephone's connection to the Avaya G430 Media Gateway, or a power management event, in which the power budget is exceeded and low priority ports are disconnected.

Identifying the problem when one phone stops working

1. Replace the telephone. If the new telephone works, the problem is with the telephone itself. If the new telephone does not work, go on to the next step.
2. See *Maintenance Procedures for Avaya Communication Manager, Media Gateways and Servers*, 03-300432 for further information.

No power on the G430

1. Check the AC power source with a voltmeter.
2. Connect the Avaya G430 Media Gateway to a different AC power source. If the G430 has power, the problem is with the original power source. If the G430 still does not work, go on to the next step.
3. Check the ALM LED on the Avaya G430 Media Gateway chassis. If it is lit, there may be a system-wide problem. Contact your project manager. See Appendix A: Front panel description on page 113.

CLI is not accessible

Check the connectivity to the G430: correct ip address and subnet on the PC attached to the G430, and the cable. Contact a certified technician if you can't resolve this problem.

NVRAM Init

Perform an NVRAM init only when you cannot access the G430, for example when the G430 resets continuously.

Important:
Performing the NVRAM init restores the G430 to its initial state with the default settings.

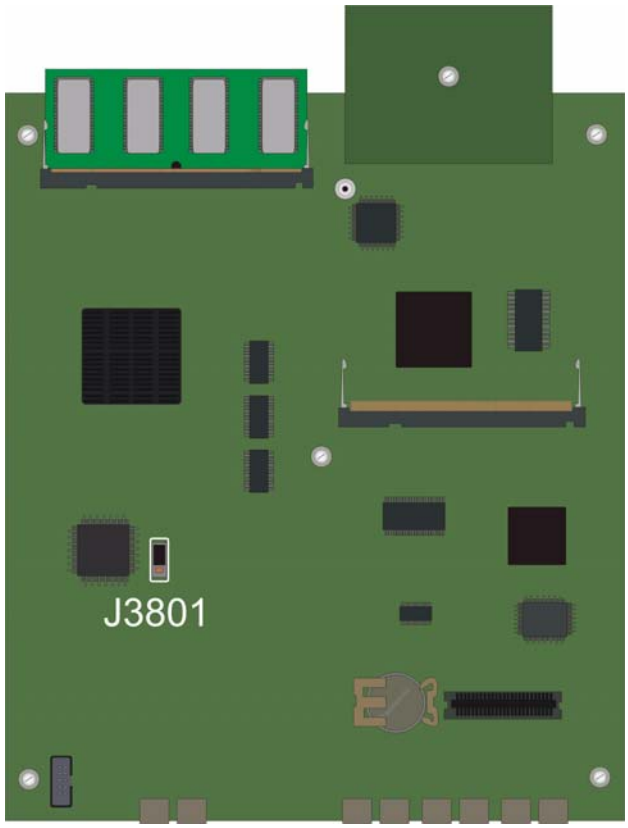
You can perform an NVRAM initialization using a jumper on the G430 motherboard.

VOLTAGE ALERT:
Disconnect the G430 from the external power source before proceeding.

ELECTROSTATIC ALERT:
Do not touch any components on the printed circuit board except when installing or removing the bridge for the jumper pins.

1. Remove the G430 cover as described in Removing the G430 cover on page 73.
2. Locate the NVRAM init jumper (jumper J3801) on the front of the G430 main board. Refer to Figure 28. Note that the jumper's two pins closest to the rear of the G430 are bridged.

Figure 28: G430 NVRAM INIT Jumper Location



3. Move the bridge on jumper J3801 so the two pins closest to the front of the G430 are bridged.
4. Place the G430 cover back on the unit, and close it with at least the top cover screw.
5. Reconnect the G430 power cable to the power connector at the rear of the G430.
6. Connect the G430 power cable into a mains socket.
7. Let the G430 operate for about 5 minutes so that it will boot and erase the current configuration. Reboot is complete when the CPU LED starts blinking.
8. Disconnect the G430 power cable from the mains power supply.
9. Disconnect the G430 power cable from the G430.
10. Unscrew the top cover screw, and remove the G430 cover.
11. Move the bridge on jumper J3801 to its initial position, in which the two pins closest to the rear of the G430 are bridged.

Important:

If you do not move the bridge on jumper J3801 to its initial position, the G430 will continue to initialize the NVRAM when it resets or is powered up.

12. Replace the G430 cover as described in Replacing the G430 cover on page 77.

Appendix A: Front panel description

You can use the front panel of the Avaya G430 Media Gateway to:

- Connect devices
- Add media modules
- View LEDs
- Reset the device
- Reset and recover from the alternate bank

The front panel of the G430 chassis and EM200 chassis without media modules

Figure 29: The G430 front panel ports and slots



Figure 30: The EM200 front panel slots



Media module slots

The G430 has three standard media module slots (V1 through V3). Each of the two optional EM200 expansion modules has two media module slots each. The slots of the EM200 connected to the EXPANSION OUT 1 connector on the rear of the G430 are slots V5 and V6, and the slots of the EM200 connected to the EXPANSION OUT 2 connector on the rear of the G430 are slots V7 and V8.

For information about the different media modules that can be housed in the media module slots, see Combination limitations on page 31 and Allocating slots on page 31.

System LEDs

Table 7: G430 System LEDs

LED	Name	Color	Indication
MDM	Modem Detected	Green	A modem is connected to the USB port
ALM	Alarm	Red	An alarm is present in the system, or an enabled compact flash has been removed
CPU	CPU	Green	OFF — A test is in progress ON — Normal operation
PWR	Power	Green	OFF — No power BLINKING — Problem with power ON — Normal operation

Table 8: EM200 System LEDs

LED	Name	Color	Indication
V5-V6		Green	The EM200 is connected to the EXPANSION OUT 1 connector on the rear of the G430
V7-V8		Green	The EM200 is connected to the EXPANSION OUT 2 connector on the rear of the G430

1 of 2

Table 8: EM200 System LEDs (continued)

LED	Name	Color	Indication
ALM	Alarm	Red	An alarm is present in the system
PWR	Power	Green	OFF — No power BLINKING — Problem with power ON — Normal operation
			2 of 2

USB ports

USB are standard USB ports, USB 1.1 and 2.0 compatible. The USB ports support the connection of:

- USB flash drive
- USB modem. See USB modems supported by the G430 on page 133 for a list of supported USB modems.

Services port (Services)

The Services port is a standard RJ-45 network port. Use the Services port to connect a laptop through a 10/100 Mbps Ethernet port to the G430 for configuration purposes.

Note:

Use a cross-over Ethernet cable.

Compact Flash Interface

The compact flash slot enables increasing the number of announcement files on the G430 from 256 to 1024, by storing them on a removable 1 GB compact flash memory card. Note however that since the announcements are played from RAM, you must also increase RAM from 256 MB to 512 MB. You can obtain an Avaya upgrade memory kit which includes both a compact flash memory card and a RAM memory card. For instructions on installing and enabling the compact flash memory card, see *Job Aid: Installing the upgrade memory kit components in the Avaya G450 and G430 Media Gateways*, 03-603203.

The yellow CARD IN USE LED adjacent to the compact flash slot indicates the state of the compact flash memory card.

Table 9: Compact Flash CARD IS USE LED states

LED	State	Meaning
CARD IN USE	Steady yellow	A compact flash card is inserted but not being used. You can safely remove the card.
	Flashing yellow	A compact flash card is in use. Do not remove the compact flash card while the LED is flashing.
	Off	A compact flash card is not inserted

Contact Closure port (CCA)

The Contact Closure port (CCA) is wired as an RJ-14 port, but uses an RJ-45 network jack. This port is used to support the G430's Contact Closure feature. The Contact Closure feature is a controllable relay providing dry contacts for various applications.

The adjunct box provides two contact closures that can be operated in either a normally closed or normally open state. The contact closures can control devices such as devices that automatically lock or unlock doors or voice recording units. The CCA port can be configured so that the connected devices can be controlled by an end device, such as a telephone. For example, a user can unlock a door by keying a sequence into a telephone keypad. For more information on Contact Closure, see Step 5: Installing the Avaya Partner Contact Closure Adjunct on page 54.

Implement the Contact Closure feature

Connect an Avaya Partner System Contact Closure Adjunct™ box to the CCA port.

Router port (ETH WAN)

ETH WAN is a standard RJ-45 network port. Use ETH WAN to connect a data device to the internal router through a 10/100 Mbps Ethernet port. The G430 serves as a router for the WAN.

Switch ports (ETH LAN)

Each ETH LAN port is a standard RJ-45 network port. Use ETH LAN to connect a data device to the switch through a 10/100 Mbps Ethernet port. You can connect an external LAN to ETH LAN.

Reset (RST) and Alternate Software Bank (ASB) buttons

RST is the reset button. ASB is the Alternate Software Bank button.

The Avaya G430 Media Gateway has two firmware banks:

- Bank A
- Bank B

Each firmware bank contains a version of the G430 firmware. These may be different versions. The purpose of this feature is to provide software redundancy. If one of the versions becomes corrupted, you can reset the G430 using the other version. This is particularly important when uploading new versions.

By default, when you turn on or reset the G430, the G430 loads firmware from Bank B. This default setting can be changed by the system administrator.

For example, if the G430 is configured to load firmware from Bank B, you can reset the G430 to load the firmware from Bank A instead.

Load firmware from a bank other than the default bank during startup

1. Press and hold the reset button.
2. Press and hold the ASB button.
3. Release the reset button.
4. Release the ASB button.

The front panel of the Avaya MM710B media module

The MM710B T1/E1 media module terminates a T1 or E1 trunk facility. For T1 connections, you can provision the MM710B to either utilize the integrated Channel Service Unit (CSU) capabilities or connect directly to an external CSU

Note:

This information also applies to the MM710.

Note:

For drop and insert, an external CSU is required.

Figure 31: The MM710B media module front panel



Note:

The six ports in the middle of the front panel are used for testing.

MM710B ports

The MM710B contains an E1/T1 port.

MM710B LEDs

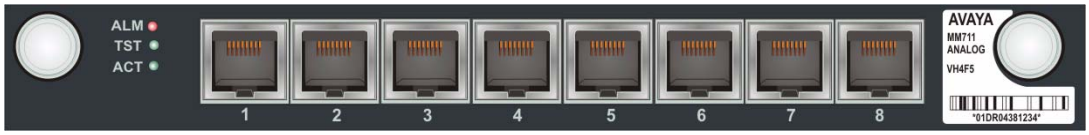
Table 10: MM710B LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	Either a test is being performed on the module via the server, or the module is performing a self-test upon initial insertion
ACT	Activity	Yellow	An E1/T1 trunk device connected to the module is in use. The light is always on if the trunk is an ISDN E1 or T1 PRI trunk, and the MM710B is not configured as the synchronization source of the G430. The light flashes at a rate of 2.8 seconds on and 0.2 seconds off if the MM710B synchronization source is configured to synchronize the G430 and the module is receiving a T1 source signal. The light flashes at a rate of 0.2 seconds on and 2.8 seconds off if the MM710B synchronization source is configured to synchronize the G430 and the T1 source is lost.
SIG	Signal	Green	The physical connection is up.

The front panel of the Avaya MM711 media module

The MM711 media module provides analog line, trunk and telephone features and functionality. The MM711 front panel includes eight universal analog ports. These ports can be used for analog telephone or fax machines, or for analog trunks.

Figure 32: The MM711 media module front panel



MM711 ports

The MM711's eight universal analog ports are labeled 1 through 8.

MM711 LEDs

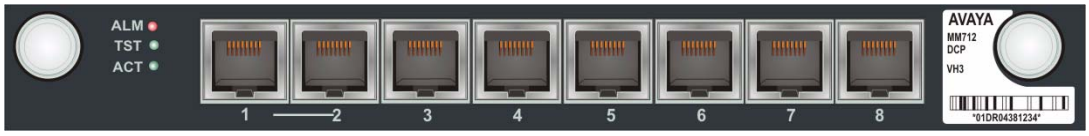
Table 11: MM711 LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	Either a test is being performed on the module via the server, or the module is performing a self-test upon initial insertion
ACT	Activity	Yellow	A device connected to the module is in use. This can include a telephone that is off the hook.

The front panel of the Avaya MM712 media module

The MM712 DCP media module includes eight DCP telephone ports. The ports support two-wire DCP telephones.

Figure 33: The MM712 media module front panel



MM712 ports

The MM712's eight DCP telephone ports are labeled 1 through 8.

MM712 LEDs

Table 12: MM712 LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	Either a test is being performed on the module via the server, or the module is performing a self-test upon initial insertion
ACT	Activity	Yellow	A device connected to the module is in use. This can include a telephone that is off the hook.

The front panel of the Avaya MM714 media module

The MM714 analog media module includes four analog telephone ports and four analog trunk ports.

Note:

The four analog trunk ports can *not* be used for analog DID trunks. Instead, the four analog line ports must be used.

Figure 34: The MM714 media module front panel



MM714 ports

The MM714's four analog telephone ports are labeled 1 through 4. These ports can also be used for DID trunks.

The MM714's four analog trunk ports are labeled 5 through 8.

MM714 LEDs

Table 13: MM714 LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	Either a test is being performed on the module via the server, or the module is performing a self-test upon initial insertion
ACT	Activity	Yellow	A device connected to the module is in use. This can include a telephone that is off the hook.

The front panel of the Avaya MM714B media module

The MM714B analog media module provides all the features provided by the MM714 (see The front panel of the Avaya MM714 media module), and in addition provides an emergency transfer relay. In the event of system failure, the MM714B provides emergency transfer relay (ETR) services by connecting trunk port 5 and line port 4.

Figure 35: The MM714B media module front panel



MM714B ports

The MM714B's four analog telephone ports are labeled 1 through 4. These ports can also be used for DID trunks.

The MM714B's four analog trunk ports are labeled 5 through 8.

MM714B LEDs

Table 14: MM714B LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	Either a test is being performed on the module via the server, or the module is performing a self-test upon initial insertion

1 of 2

Table 14: MM714B LEDs (continued)

LED	Name	Color	Indication
ACT	Activity	Yellow	A device connected to the module is in use. This can include a telephone that is off the hook.
ETR	ETR	Green	The Emergency Transfer Relay (ETR) feature has been activated. This feature provides an emergency link between the telephone connected to the line port 4 and the trunk connected to trunk port 5 if power is disconnected from the G430 or if the G430 becomes unregistered from its Media Gateway Controller (MGC) Turning on ETR manually using the **`set etr manual-on`** CLI command also lights this LED..
			2 of 2

The front panel of the Avaya MM716 media module

The MM716 media module front panel has a 25-pair amphenol connector supporting 24 analog line ports. These ports can be configured as DID trunks with either wink start or immediate start.

The MM716 is compatible with Avaya CM version 2.0 and higher, and G430 firmware version 25.0.0 and higher.

Figure 36: The MM716 media module front panel



MM716 ports

The MM716 contains a single 25-pair amphenol connector, which can be connected by an amphenol cable to a breakout box or punch down block containing RJ-45 or RJ-11 jacks, as needed. You can attach up to 24 devices (analog telephones, trunks, modems, or fax machines) to these jacks.

Table 15: 25-pair amphenol connector pinout

Station port	Cable pair	
1	White	Blue
2	White	Orange
3	White	Green
4	White	Brown
5	White	Slate
6	Red	Blue
7	Red	Orange
8	Red	Green
9	Red	Brown
10	Red	Slate
11	Black	Blue
12	Black	Orange
13	Black	Green
14	Black	Brown
15	Black	Slate
16	Yellow	Blue
17	Yellow	Orange
18	Yellow	Green
19	Yellow	Brown
20	Yellow	Slate

1 of 2

Table 15: 25-pair amphenol connector pinout (continued)

Station port	Cable pair	
21	Violet	Blue
22	Violet	Orange
23	Violet	Green
24	Violet	Brown
OPEN	Violet	Slate
		2 of 2

MM716 LEDs

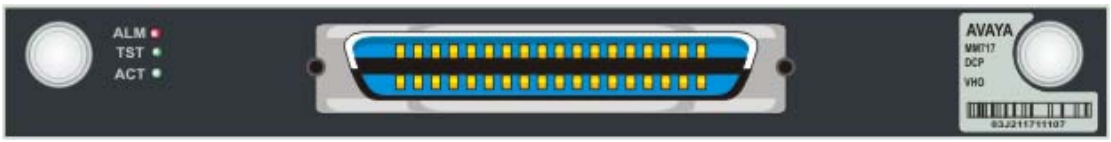
Table 16: MM716 LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	Either a test is being performed on the module via the server, or the module is performing a self-test upon initial insertion
ACT	Activity	Yellow	A device connected to the module is in use. This can include a telephone that is off the hook.

The front panel of the Avaya MM717 media module

The MM717 high density DCP media module front panel has a 25-pair amphenol connector supporting 24 Digital Communications Protocol (DCP) ports. To use the MM717 media module, connect an amphenol cable to the port and to either a breakout box or a punch down block containing RJ-45 or RJ-11 jacks, as needed. You can attach up to 24 two-wire DCP telephones to these jacks. The MM717 does not support four-wire DCP telephones.

Figure 37: The MM717 media module front panel



MM717 ports

The MM717 contains a single 25-pair amphenol connector, which can be connected by an amphenol cable to a breakout box or punch down block containing RJ-45 or RJ-11 jacks, as needed.

Table 17: 25-pair amphenol connector pinout

Station port	Cable pair	
1	White	Blue
2	White	Orange
3	White	Green
4	White	Brown
5	White	Slate
6	Red	Blue
7	Red	Orange
8	Red	Green
9	Red	Brown
10	Red	Slate
11	Black	Blue
12	Black	Orange
13	Black	Green
14	Black	Brown
15	Black	Slate
16	Yellow	Blue

1 of 2

Table 17: 25-pair amphenol connector pinout (continued)

Station port	Cable pair	
17	Yellow	Orange
18	Yellow	Green
19	Yellow	Brown
20	Yellow	Slate
21	Violet	Blue
22	Violet	Orange
23	Violet	Green
24	Violet	Brown
OPEN	Violet	Slate
		2 of 2

MM717 LEDs

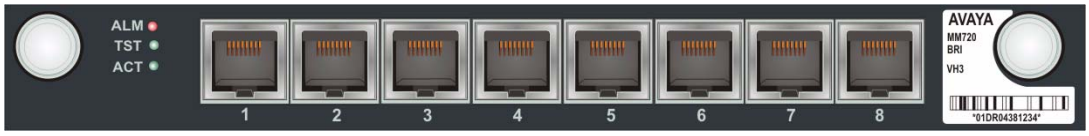
Table 18: MM717 LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	Either a test is being performed on the module via the server, or the module is performing a self-test upon initial insertion
ACT	Activity	Yellow	A device connected to the module is in use

The front panel of the Avaya MM720 media module

The MM720 ISDN BRI media module contains eight 4-wire S/T ISDN BRI ports. These ports interface to the central office at the ISDN T reference point.

Figure 38: The MM720 media module front panel



MM720 ports

The MM720's eight ISDN BRI ports are labeled 1 through 8.

MM720 LEDs

Table 19: MM720 LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	Either a test is being performed on the module via the server, or the module is performing a self-test upon initial insertion
ACT	Activity	Yellow	A trunk connected to the module is in use. In CM 3.0 or higher, the LED could alternatively indicate that a telephone connected to the module is in use.

The front panel of the Avaya MM722 media module

The MM722 ISDN BRI media module provides two 4-wire S/T ISDN BRI (Basic Rate Interface) 2B+D access ports with RJ-45 jacks.

Figure 39: The MM722 media module front panel



MM722 ports

The MM722 contains two ISDN BRI ports.

MM722 LEDs

Table 20: MM722 LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	Either a test is being performed on the module via the server, or the module is performing a self-test upon initial insertion
ACT	Activity	Yellow	A trunk connected to the module is in use. In CM 3.0 or higher, the LED could alternatively indicate that a telephone connected to the module is in use.

Appendix B: Technical specifications

This appendix provides technical specifications for the G430, for the EM200, for compatible power cords, and for USB modem support.

G430 Media Gateway specifications

The following table provides detailed information on the physical dimensions and tolerances of the G430 Media Gateway.

Table 21: Avaya G430 Media Gateway specifications

Description	Value
Height	2.62 in. (66.5 mm)
Width	19 in. (482.6 mm)
Depth	12.8 in. (325 mm)
Weight of empty chassis	under 11 pounds (under 5 Kg)
Weight of chassis with basic configuration	Between 13 and 14 pounds (between 6 and 7 kg)
Ambient working temperature	32° to 104°F (0° to 40°C)
Operation altitude	up to 10,000 ft. (3000 m)
Front Clearance	12 in. (30 cm)
Rear Clearance	18 in. (45 cm)
Humidity	10-90% relative humidity, non-condensing
Power rating	90V-264V AC, 48-62 Hz
BTU	800 BTU/h
Max current	3 A

EM200 specifications

The following table of technical specifications provides detailed information on the physical dimensions and tolerances of the EM200 expansion module:

Table 22: EM200 specifications

Description	Value
Height	2.62 in. (66.5 mm)
Width	19 in. (482.6 mm)
Depth	12.8 in. (325 mm)
Weight of empty chassis	under 11 pounds (under 5 kg)
Weight of chassis with media modules and brackets	13 pounds (6 kg)
Ambient working temperature	32° to 104°F (0° to 40°C)
Operation altitude	up to 10,000 ft. (3000 m)
Front Clearance	12 in. (30 cm)
Rear Clearance	18 in. (45 cm)
Humidity	10-90% relative humidity, non-condensing
Power rating	90V-264V AC, 48-62 Hz
BTU	430 BTU/h
Max current	3 A

Power cord specifications

Following are specifications for power cords suitable for use with the G430.

For North America: The cordset must be UL Listed/CSA Certified, 16 AWG, 3-conductor (3rd wire ground), type SJT. One end is to be terminated to an IEC 60320, sheet C13 type connector rated 10A, 250V. The other end is to be terminated to either a NEMA 5-15P attachment plug for nominal 125V applications or a NEMA 6-15P attachment plug for nominal 250V applications.

For Outside North America: The cord must be VDE Certified or Harmonized (HAR), rated 250V, 3-conductor (3rd wire ground), 1.0 mm^2 minimum conductor size. The cord is to be terminated at one end to a VDE Certified/CE Marked IEC 60320, sheet C13 type connector rated 10A, 250V and the other end to a 3-conductor grounding type attachment plug rated at a minimum of 10A, 250V and a configuration specific for the region/country in which it will be used. The attachment plug must bear the safety agency certifications mark(s) for the region/country of installation.

USB modems supported by the G430

- USRobotics USB modem, model 5637
- Multitech USB modem, model MT5634ZBA-USB-V92

USB modems supported by the S8300

- USRobotics USB modem, model 5637
- Multitech USB modem, model MT5634ZBA-USB-V92
- Multitech USB modem, model MT9234-ZBA

Appendix C: Running the Avaya Installation Wizard (Avaya IW)

The Avaya IW is a web-based installation wizard that is used with the Avaya G430 Media Gateway to perform initial configuration tasks and to upgrade software and firmware. The Avaya IW is designed for use with systems that contain an S8300 Server, operating in either ICC or LSP mode. You can use Avaya IW to configure the Avaya G430 Media Gateway or to upgrade an installed S8300 with new Avaya Aura Communication Manager (CM) software and/or G430 firmware.

See *Job Aid: Avaya Installation Wizard*, 555-245-754 for information on the Avaya Installation Wizard.

Appendix D: Running the Gateway Installation Wizard (GIW)

If you did not install an S8300 in the G430, you can use the Gateway Installation Wizard (GIW) to perform the configurations required to complete the installation. GIW prompts you for all the configurations required to complete the installation. If you have an EPW (see Obtaining the Electronic Preinstallation Worksheet (EPW) on page 21), you will be able to upload configuration parameters from the EPW to GIW as part of your GIW session.

GIW includes the option to enable a modem connected to the S8300. This appendix describes how to run GIW, and how to connect and test a modem if you choose to enable the modem.

Note:

If you run GIW, ensure that services can login to the system using USB modem after you run the GIW.

Running the Gateway Installation Wizard (GIW)

Running the GIW performs a basic configuration of the G430. The configuration can include:

- Configuring the Primary Management Interface (PMI)
- Setting SNMP communities and trap destinations
- Upgrading firmware
- Enabling a modem on the G430

Performing a basic configuration of the G430

1. Prepare a PC with a CD-ROM drive and a TFTP server on the network. This may be needed for installing software and firmware upgrades.

   Note:

   When uploading firmware from the S8300 using TFTP, you may need to enable TFTP service in the Set LAN Security parameters of your web server.

Note:

Firmware upgrades for the G430 and media modules can either be installed from CD or downloaded from the Web. For information about downloading firmware upgrades from the Web to the TFTP server, see Downloading G430 firmware files to a local TFTP server on page 91.

2. Download GIW (Gateway Installation Wizard) from the Avaya Support website (support.avaya.com/avayaiw) to the laptop computer. The laptop should be running Windows 2000, or Windows XP to support GIW.
3. Set the laptop's TCP/IP properties as follows:
   - IP address: 192.11.13.5
   - Subnet mask: 255.255.255.252
   - Disable DNS service
   - Disable WINS Resolution
4. Disable the proxy server in the laptop’s Internet browser settings.
5. Connect the laptop computer to the G430 Services port, using an Ethernet cable.
6. From your laptop computer, double-click the GIW icon to run GIW. The Overview screen appears.
7. Click **Continue**. The Gateway Connection Details screen appears.
8. Enter the connection details:
   a. Select **Select if this is a G430 Gateway**.
   b. Enter your Username and Password
9. Click **Continue**. The Initializing the Components screen appears.
10. Select **Initialize the Gateway Installation Session**.
11. Click **Continue**. The Import Electronic Preinstallation Worksheet screen appears.
12. If you have an EPW on your laptop (see Obtaining the Electronic Preinstallation Worksheet (EPW) on page 21), check **Import EPW**. If you are using GIW to only upgrade files, verify that **Import EPW** is unchecked.
13. Browse to the EPW file on your laptop. Any values that are included in the EPW will appear as default values from now on as you move through this wizard.
14. Click **Continue**. The IP Addresses screen appears.

    The IP Addresses screen displays automatically detected information about the G430, such as what media modules are installed in the media modules slots.
15. If you are using GIW only to upgrade firmware, continue with step 25.
16. Click  in the Action column. The PMI screen appears.

17. In the PMI screen, specify the details of the Primary Management Interface (PMI) for the G430. The PMI is used as the IP address of the G430 for specific management functions. If you do not know which interface to designate as the PMI, check with your project manager.
18. Click **Continue**. The SNMP V1 screen appears.
19. In the SNMP V1 screen, specify SNMP V1 Community Strings for **Read Only** and **Read Write** access.
20. Click **Continue**. The SNMP V3 screen appears.
21. If you want to configure an SNMP V3 user on the G430:
    a. In the **User Name** field, enter a string of up to 32 characters representing the SNMP V3 user.
    b. In the **Authentication Protocol** field, select the authentication protocol by which the SNMP V3 user should be authenticated (SHA1 or MD5).
    c. In the **Authentication Password** field, enter a string of between 8 and 64 characters specifying the user's authentication password. The authentication password is transformed using the authentication protocol and the SNMP engine ID to create an authentication key.
    d. In the **Re-enter Authentication Password** field, enter the authentication password again for verification.
    e. In the **Privacy Password** field, enter a string of between 8 and 64 characters specifying the SNMP V3 user's privacy password.
    f. In the **Re-enter Privacy Password** field, enter the privacy password again for verification.
22. Click **Continue**. The IP Addresses - Media Gateway Controller List screen appears.
23. In the Media Gateway Controller List screen:
    a. Specify the IP address of the primary Media Gateway Controller (MGC) in the first IP address box.
    b. Specify the IP addresses of up to three additional MGCs, optionally, in the subsequent boxes.
    c. Specify Transition Point information.
    d. Click **Ping Test** to test the accessibility of each MGC.
24. Click **Continue**. You return to the IP addresses screen.
25. Click **Continue**. The Firmware screen appears.
26. In the Firmware screen:
    a. Upload any firmware upgrades you need to install to your TFTP server.
    b. In the **TFTP Address** field, enter the address of your TFTP server.

c. In the **TFTP Directory** field, enter the name of the directory on the TFTP server in which the upgrade files are located.

d. In the table, check the **Select** box for all firmware components you want to upgrade. The current version of each component is listed to help you confirm the need for upgrade.

e. Enter the file name of each firmware upgrade file you want to install in each line of the table where you checked the **Select** box.

27. Click **Continue**. The firmware is upgraded and the Change Master Key - Optional screen appears. The master key is used to encrypt gateway secrets (passwords, etc.) in the gateway configuration file.
28. If you want to change the master key, enter the new master key passphrase in the Create Master Key field, and then confirm by entering it again in the Confirm Master Key field. A new master key is generated from the passphrase.
29. Click **Continue**. The Gateway Authentication screen appears.
30. If you have a service contract, the G430 is shipped with an authentication file. This authentication file is required for Avaya services personnel to allow them secure remote access to the gateway.
31. Click **Continue**. The Field Replaceable Unit (FRU) Status screen appears. View the status of the Field Replaceable Units detected in the G430.
32. Click **Continue**. The TFTP Server screen appears. The TFTP Server screen enables you to upload firmware and configuration files for IP phone upgrades to the G430 TFTP server.
33. If you want to upload configuration and firmware files for IP phones to the G430 TFTP Server, do the following:

    a. In the **Server IP Address** field, enter the IP address of the machine hosting the files that are to be uploaded.

    b. Select the file transfer protocol (TFTP, FTP, or SCP) you want to use to upload the files from the host machine. TFTP is selected by default.

    The use of the SCP protocol is limited to copying files of 1 MB or less. Therefore, an SCP server can be used for copying the script files, which do not exceed 128 KB, but cannot be used for copying image files.

    c. If you selected FTP or SCP, enter the username and password in the **Username** and **Password** fields, and re-enter the password for confirmation in the **Re-enter Password** field.

34. Click **Continue**.
35. In the **Select** column, check any files you wish to upload.

Note:

If you selected SCP as your upload protocol, the checkboxes for the phone images are disabled. If a green circled checkmark is displayed in the Uploaded column, the file has already been uploaded.

36. Click **Continue**. The files are uploaded and the G430 Modem Type Selection screen appears. If you are using GIW only to upgrade firmware, click **Continue** until you reach the Finish Up screen. Go to step 42.
37. If you do not need to connect a modem to the G430, select **None**. If you do need to connect a modem to the G430, select **USB Modem**.
38. Click **Continue**. The modem configuration (Serial or USB) screen appears.
39. To configure the modem:
    a. In the **PPP IP Address** field, enter the RAS IP address of the modem obtained using the ART tool. See Running the Automatic Registration Tool (ART) for the RAS IP address on page 20.
    b. Enter the PPP Subnet Mask.
    c. Select the authentication method:
       - If you have an Avaya Service contract, check **Enable ASG Authentication** to enable remote access to the device.
       - If you do not have an Avaya Service contract:
         – Check **Enable CHAP Authentication**.
         – In the **CHAP Secret** field, enter the CHAP secret key obtained using the ART tool. See Running the Automatic Registration Tool (ART) for the RAS IP address on page 20.
         – In the **Confirm CHAP Secret** field, re-enter the CHAP secret key.
40. Click **Continue**. The Change Root Password screen appears.
41. If you would like to change the password on the G430 Media Gateway, enter the current password in the Current Password field, enter a new password in the New Password field, and re-enter the new password in the Confirm New Password field.
42. Click **Continue**. The Finish Up screen appears.

    Follow the on-screen instructions if you want to save the installation log file. Further configurations, as described in this screen, can now be performed either remotely, via a modem that you enabled with GIW, or locally.

Connect a USB modem, if necessary

If you enabled a USB modem on the G430 during your GIW session, you can now connect the modem.

1. Connect a USB modem to a working telephone line.

Note:

See USB modems supported by the G430 on page 133 for a list of supported USB modems.

2. Connect one end of a USB cable to the modem.
3. Connect the other end of the USB cable to a USB port on the G430 front panel.

Test the modem connection

If the modem is successfully initialized, the MDM LED on the G430 front panel lights.

Testing the modem

If you connected a modem, verify that the MDM LED is lit, and then dial into the modem to check that you can authenticate to the modem.

Appendix E: Power supplies and adjunct systems

This appendix provides information and wiring examples of installation procedures for various telephone and console power supplies.

In addition, you may need to install one or more adjunct systems or devices. Follow the instructions in:

- Avaya Aura Communication Manager messaging application on page 145
- Call center on page 145

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.

Typical adjunct power connections

The 400B2 adapter is convenient for connecting local -48 VDC power to a modular plug. See Figure 40.

See *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151, for detailed power supply information and installation procedures.

Figure 40: 400B2 Adapter Connecting to a Modular Plug

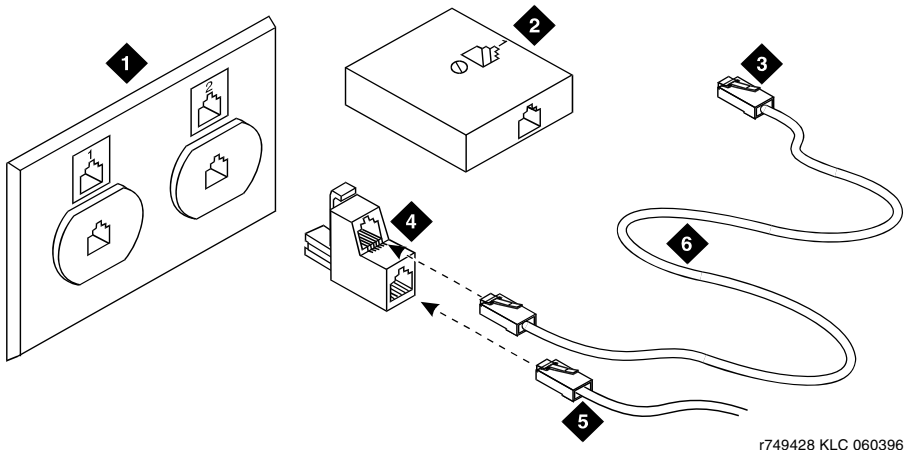


Figure notes:

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 41 shows typical connection locations for adjunct power.

Figure 41: Example Adjunct Power Connections

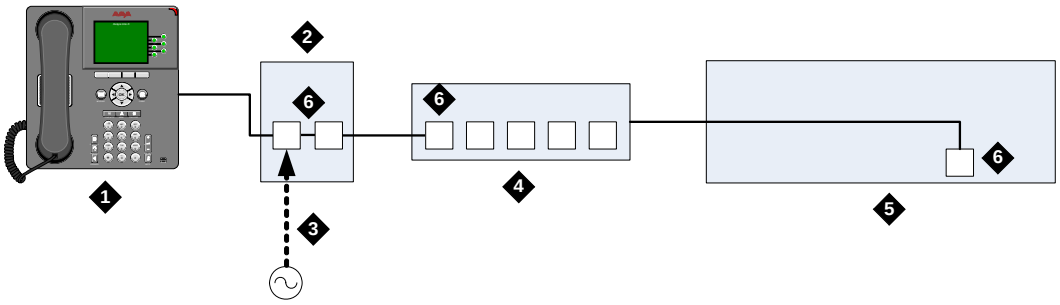


Figure notes:

1. **Avaya IP telephone**
2. **Power brick**
3. **AC power inlet**
4. **Switch**
5. **G430**
6. **LAN port**

Avaya Aura Communication Manager messaging application

The Avaya Aura™ Communication Manager Messaging application (formerly known as IA770) runs as a process on the S8300 Server. Without the need for additional hardware, the software processes touchtones, converts messages to the G.711 format, and converts text to speech.

Call center

The S8300 Server provides an excellent solution for a small call center. The S8300 Server with one or more G430 Media Gateways supports the following call center capabilities:

- All three Avaya call center packages:
  - Avaya Call Center Basic
  - Avaya Call Center Deluxe
  - Avaya Call Center Elite
- Avaya G430 announcement software

About Avaya G430 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 G430. You can substantially increase the number of supported announcement files on the gateway if you install a compact flash and increased RAM (see Installing the upgrade memory kit on page 79) and configure the G450 in the media-gateway form.

Appendix F: Information Checklists

This appendix can be used as an aid for collecting necessary information for the installation of an Avaya G430 Media Gateway Media Gateway.

The following lists are provided:

- Installer's Checklist: Tools, software, laptop settings, customer network information
- Serial Number and Login Information: Serial number of the G430 and login/passwords for various access methods
- Quick Setup for G430 Media Gateway Processor (MGP): IP addresses and setup commands for the MGP
- Installation Site Information: Customer and site contact information

Installer's Checklist

	Tools
	laptop with 32 MB RAM
	40 MB available disk space
	RS-232 port connector or Ethernet interface
	cross-over Ethernet cables
	direct Ethernet cable
	USB flash drive (optional)
	screwdriver
	Software
	Windows 95/98/ME/XP/NT/2000/Vista operating system
	FTP server program. TFTP server program and SCP server program are recommended
	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
	communications properties: 9600 baud rate; no parity; 8 data bits, 1 stop bit; no flow
	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

G430 Serial Number

Logins

	Name & Password
S8300 Server	
G430 Media Gateway	
SSO Authentication Login	
ftp	anonymous email address
Communication Manager	

Quick Setup for G430 Media Gateway Processor (MGP)

Task	CLI Command	Requested Fields	Information to enter
Define a Primary Management Interface (PMI)	Enter the context of the interface which you want to set as the Primary Management Interface (PMI). For example: **`interface vlan`**	***`vlan id`***	
	In the context of the interface, assign an IP address and subnet mask to the interface: **`ip address`**	***`IP address`***	
		`netmask`	
	In the context of the interface, define this interface as the PMI **`pmi`**		
Configure the ICC-VLAN **Note**: By default, the ICC-VLAN is 1. Therefore configure the ICC-VLAN only if you wish to configure it for a VLAN other than 1.	Create a vlan and enter its configuration context: **`interface vlan`**	***`vlan id`***	
	In the context of the vlan interface, set the current vlan as the icc-vlan: **`icc-vlan`**		
	Set the VLAN ID of a LAN port (10/5 or 10/6) to the VLAN number of the ICC-VLAN: **`set port vlan`**	***`vlan id`***	
		`module number`	
		`port number`	
Define the CLI prompt	**`hostname`**	***`hostname`***	
Define a default gateway	**`ip default-gateway`**	***`gateway IP address`***	
Create a list of valid Media Gateway Controller(s)	**`set mgc list`**	***`IP address1`***	
		`IP address2`	
		`IP address3`	
		`IP address4`	
Display device information	**`show system`**		

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	

Appendix G: Equipment List

The following lists contain information necessary for ordering Avaya G430 Media Gateway, EM200, and Avaya S8300 Server equipment.

Note:

If ordering parts, use the 9-digit "Comcode" numbers, not the 6-digit numbers.

Table 23: Equipment List: Avaya G430 Media Gateway

Avaya G430 Media Gateway

The Avaya G430 Media Gateway is a 19-inch 1.5u rack-mountable device. The G430 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 three Media Module Bays, and can be extended to provide up to seven Media Module Bays. The Avaya G430 Media Gateway is designed to offer options and scalability. You can mix and match media modules, as well as add additional Avaya G430 Media Gateways as they grow in size.

Avaya G430 Media Gateway Comcodes (for Services Ordering Only)

Comcode	Number of Items	Description
700469273	1	G430 chassis
700017932	1	Rack Mount screw set for attaching the ears to the rack
700438997	2	Rack Mount Ears
700439003	1	Cable Management Ear
700305535	15	Rack Mount screw set for attaching the ears to the chassis
700318421	4	Feet
700318397	1	Tech Laptop Cable
700336597	8	Media Module Blanks
700336621	2	Low-Profile blanks (S8300)
700236680	1	Grounding Kit for multiple G430s in a 19 inch rack

1 of 2

Table 23: Equipment List: Avaya G430 Media Gateway (continued)

Avaya G430 Media Gateway	
Avaya G430 Media Gateway Comcodes for Customer and Services ordering	
Comcode	**Description**
700432503	80 channels DSP daughterboard
700432511	20 channels DSP daughterboard
700460660	10 channels DSP daughterboard
700469273	G430 Chassis
700457013	Upgrade memory kit
	2 of 2

Table 24: Equipment List: EM200 Expansion Module

EM200 Expansion Module
The EM200 Expansion Module is a 19-inch 1.5u rack-mountable device. The EM200 houses two Media Module Bays, and serves as an extension to the Avaya G430 Media Gateway. You can connect up to two EM200 modules to an Avaya G430 Media Gateway.

EM200 Comcodes (for Services Ordering Only)

Comcode	Number of Items	Description
700460538	1	EM200 chassis
700017932	1	Rack Mount screw set for attaching the ears to the rack
700438997	2	Rack Mount Ears
700439003	1	Cable Management Ear
700305535	15	Rack Mount screw set for attaching the ears to the chassis
700318421	4	Feet
700476062	1	EM200 Stacking Cable
700336597	8	Media Module Blanks
700236680	1	Grounding Kit for multiple EM200s in a 19 inch rack

Table 25: Equipment List: G430 Media Gateway and EM200 Power Cords

G430 Media Gateway and EM200 Power Cords
Supplies Power to the G430 Media Gateway chassis and EM200 chassis. One cord per chassis is required, and there are various cords depending on the power required for the country in which the unit will be installed.
When you order this material code, a descriptive attribute will be required; the attributes are:

Attribute	Option	Comcode: Description
CRD	30	405362641: PWR CORD 9X10IN USA 17505

1 of 2

Table 25: Equipment List: G430 Media Gateway and EM200 Power Cords (continued)

G430 Media Gateway and EM200 Power Cords		
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

2 of 2

Table 26: Equipment List: Avaya S8300C Server

Server
S8300C Server
The Avaya S8300C Server is an Intel™-based server complex that carries: ● Administration and maintenance provisioning software ● Web serve ● Linux OS ● H.248 Media Gateway Signaling Protocol ● CCMS messages tunneled over H.248 Signaling Protocol ● TFTP server The S8300D Server can act as the primary server of the G430 Media Gateway, or it can serve as a local survivable processor for remote/branch customer locations.
Comcode (for Services Ordering Only): 700407810

Table 27: Equipment List: Avaya S8300D Server

Server
S8300D Server
The Avaya S8300D Server is an Intel™-based server complex that carries: • Administration and maintenance provisioning software • 8 GB Internal Solid State Drive (SSD) • Web serve • Linux OS • H.248 Media Gateway Signaling Protocol • CCMS messages tunneled over H.248 Signaling Protocol • TFTP server The S8300D Server can act as the primary server of the G430 Media Gateway, or it can serve as a local survivable processor for remote/branch customer locations.
Comcode (for Services Ordering Only): 700407810

Table 28: Equipment List: Avaya S8300D Server

Server
S8300D Server
The Avaya S8300D Server is an Intel™-based server complex that carries: • Administration and maintenance provisioning software • Web serve • Linux OS • H.248 Media Gateway Signaling Protocol • CCMS messages tunneled over H.248 Signaling Protocol • TFTP server The S8300D Server can act as the primary server of the G430 Media Gateway, or it can serve as a local survivable processor for remote/branch customer locations.
Comcode (for Services Ordering Only): 700447675

Table 29: Equipment List: Media Modules

Media Modules

MM710 T1/E1 Media Module	Comcodes (for Services Ordering Only): 700394737, 700439250, 700466634

The MM710 T1/E1 media module offers the combined features of a DEFINITY DS1 circuit pack and includes the following:

- A built-in CSU
- AMI-BASIC
- Both A-law for E1 and μ -law for T1
- Line Coding: AMI, ZCS, B8ZS for T1 and HDB3 or AMI for E1
- Stratum 3 Clock compatibility
- Trunk signaling for supporting US and International CO trunks and tie trunks as currently in existence

The MM710 T1/E1 media module supports the universal DS1 conforming to 1.544 Mbps T1 standard and 2.048 Mbps E1 standard.

ISDN PRI is also supported for T1 or E1 revenue-associated option. The MM710 is RoHS compliant.

MM710B T1/E1 Media Module	Comcodes (for Services Ordering Only): 700394737, 700439250, 700466634

The MM710B T1/E1 media module offers the combined features of a DEFINITY DS1 circuit pack and includes 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 MM710B T1/E1 media module supports the universal DS1 conforming to 1.544 Mbps T1 standard and 2.048 Mbps E1 standard.

ISDN PRI is also supported for T1 or E1 revenue-associated option. The MM710B is RoHS compliant.

1 of 4

Table 29: Equipment List: Media Modules (continued)

Media Modules		
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: 700406101	Apparatus Code: None	Required for any customer with a maintenance contract and an MM710 or MM7110B T1/E1 media module. Highly recommended for other customers to avoid expensive technician visits.
MM711 Analog Media Module	Comcodes (for Services Ordering Only): 700394661, 700466626	
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. The MM711 Analog media module also allows connectivity of analog, tip/ring devices such as single line telephones, modems or group 3 fax machines. Each port may be configured as either a trunk interface or a station interface. Also included is support for caller ID signaling, ring voltage generation for a variety of international frequencies and cadences, and administrable line termination styles. The MM711 is RoHS compliant.		
MM714 Analog Media Module	Comcode (for Services Ordering Only): 700395221	
The MM714 Analog media module supports four analog stations and four CO trunks. Analog DID trunk connections are to be associated with the ports labeled "Line" and not "Trunk". The MM714 is RoHS compliant.		
MM714B Analog Media Module	Comcodes (for Services Ordering Only): 700453889, 700466618	

2 of 4

Table 29: Equipment List: Media Modules (continued)

Media Modules
The MM714B Analog media module supports four analog stations and four CO trunks, as well as an Emergency Transfer Relay between a line port and a trunk port. Analog DID trunk connections are to be associated with the ports labeled "Line" and not "Trunk". The MM714B is RoHS compliant.

MM712 DCP Media Module	Comcode (for Services Ordering Only): 700394745
The MM712 DCP media module allows connectivity of up to eight 2-wire DCP voice terminals. MM712 does not support 4-wire DCP telephones. Signal timing specifications for the MM712 support TDM Bus Timing in receive and transmit modes. The G430 Media Gateway supplies only +5 VDC and –48 VDC to the MM712 media module. Any other required voltages must be derived on the module. Loop range secondary protection is provided on the MM712. The MM712 is also self-protecting from an over current condition on a tip and ring interface. The MM712 is RoHS compliant.	

MM716 24 port Analog Media Module	Comcodes (for Services Ordering Only): 700394703, 700466642
The MM716 provides 24 analog ports supporting telephones, modem, and fax. These ports can also be configured as DID trunks with either wink-start or immediate-start. The 24 ports are provided via a 25-pair RJ21X amphenol connector, which can be connected by an amphenol cable to a breakout box or punch down block. The MM716 is RoHS compliant.	

MM717 24 port DCP Media Module	Comcode (for Services Ordering Only): 700394711
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. The MM717 is RoHS compliant.	

MM720 BRI Media Module	Comcode (for Services Ordering Only): 700394752

3 of 4

Table 29: Equipment List: Media Modules (continued)

Media Modules
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 eight ports on the MM720 BRI media module can support one integrated voice/data endpoint or up to two BRI stations and/or data modules. Supported endpoints must conform to AT&T BRI, World Class BRI, or National ISDN NI1/NI2 BRI standards. The MM720 BRI media module provides -40 volt phantom power to the BRI endpoints. The MM720 is RoHS compliant.

MM722 2-port BRI Media Module	Comcode (for Services Ordering Only): 700395239
The MM722 BRI media module provides two 4 wire S/T ISDN BRI 2B+D access ports with RJ-45 jacks. Each port interfaces to the central office at the ISDN T reference point. Information is communicated in the same manner as for the MM720. The MM722 is RoHS compliant.	

Index

Numerical

400B2 Adapter 144

A

Access, RFA 18
Accessories box, contents 23
Adjunct
  power connections 143
    end-to-end 144
After installation
  overview 63
  testing
    connectivity 63
    LSP failover 64
    overview 63
    telephones 63
    trunks 63
Allocating media module slots 31
Alternate Software Bank button 117
Amphenol cable, attaching to MM716 or MM717 . . . 51
Analog
  port, connecting analog telephone to 46
  telephone, connecting to analog port 46
  trunk
    connecting 49
    ordering 69
Announcements, gateway 145
Approved grounds 38
ART (Automatic Registration Tool), running for RAS IP address 20
ASB button 117
ASG authentication
  enabling in GIW 56, 141
  installing authentication file
    in GIW 140
Attaching
  amphenol cable to MM716 or MM717 51
  analog telephone to analog port 46
  analog trunk 49
  and enabling a modem
    gateway without S8300 55
    general description 55
  and enabling a USB modem
    gateway with S8300 58
  Avaya Partner Contact Closure Adjunct 54
  BRI stations to ISDN port 44
  chassis to wall or rack 25
  circuit protection devices 52
  Coupled Bonding Conductor (CBC) 53
  data and voice devices 43
  DCP telephones 48
  E1/T1
    trunk 50
  endpoint devices 43
  Ethernet WAN link 53
  external router 53
  ground conductors 37
  IP telephone to gateway 44
  ISDN trunk 50
  modem to gateway without S8300 55
  safety ground 40
  switch or network data port 43
  USB modem to gateway with S8300 58
AUDIX
  Avaya Aura Communication Manager 145
Authentication
  CHAP, enabling in GIW 141
  file
    for CM
      obtaining 19
    for gateway
      installing in GIW 140
Automatic Registration Tool
  see ART
Avaya Aura Communication Manager (CM)
  version requirements for LSP 19
Avaya Aura Communication Manager Messaging 145
Avaya Gateway Manager, upgrading Java applet via FTP/TFTP 88
Avaya Installation Wizard (IW)
  configuration, initial 135
  description 61
  gateway
    firmware, upgrading 86
  overview 135
Avaya Navy Shipboard Services 25
Avaya Partner Contact Closure Adjunct 54
Avaya Software Update Manager 85

B

Backing up the gateway to USB mass storage device 107
Before installation
  environmental verification 22

grounding verification 22
power verification 22
read planning documentation 17
required equipment 17
site requirements 22
unpacking 24
Boot banks 117
Box inventory 23
Brackets, mounting
for rack
attaching 27
checks before 27
types of 25
with cable guides 26
without cable guides 26
for wall 28
attaching to gateway 28
BRI stations, connecting to ISDN port 44
Buttons
ASB 117
RST 117

C

Cable guides on mounting bracket 25, 26
Call center 145
gateway announcements 145
CBC (Coupled Bonding Conductor) 53
installing 54
CCA port 116
CD-ROM drive, upgrading software 59
CHAP authentication
enabling 56
enabling in GIW 141
Chassis
front panel description 113
installation
see Gateway chassis installation
Checking
available number of power outlets 22
environment before installing 22
grounding 22
Circuit protection, installing 52
CLI
commands for upgrading firmware
via a USB device 94
via FTP/TFTP 88
description 61
troubleshooting 110
upgrading gateway firmware
via FTP/TFTP 88
via USB device 93
CM
authentication file
downloading to laptop 19
license file
downloading to laptop 19
Combination limitations for media modules 31
Command Line Interface
see CLI
Commands
copy ftp EW_archive 88
copy ftp module 88
copy ftp phone-image 100
copy ftp phone-script 100
copy ftp SW_imageA 89
copy ftp SW_imageB 89
copy running-config startup-config 100
copy scp phone-script 100
copy tftp EW_archive 89
copy tftp module 89
copy tftp phone-image 100
copy tftp phone-script 100
copy tftp SW_imageA 89
copy tftp SW_imageB 89
copy usb EW_archive 94
copy usb module 94
copy usb phone-image 100
copy usb phone-script 100
copy usb SW_imageA 94
copy usb SW_imageB 94
erase phone-image 101
ip tftp-server file-system size 100
reset 100
save translation lsp 65
show application-memory 100
Compact flash
port 115
Compact flash memory card
hot insertion 80
inserting 80
removing 81
Computer
downloading gateway firmware to local 94
Conditions good for installation 22
Configuration
files
upgrading IP phone, overview 97
gateway 61
basic 137
initial in GIW 137
initial in IW 135
limitations of media modules 31
telephone 68
telephone software, recording information for . . . 68
trunk 69
trunk software, recording information for 70
Connecting
analog telephone to analog port 46
analog trunk 49

and enabling a modem
gateway without S8300 . . . 55
general description . . . 55
USB
gateway with S8300 . . . 58
gateway without S8300 . . . 55
Avaya Partner Contact Closure Adjunct . . . 54
BRI stations to ISDN port . . . 44
circuit protection devices . . . 52
computer to Services port . . . 43
Coupled Bonding Conductor (CBC) . . . 53
data and voice devices . . . 43
DCP telephones . . . 48
E1/T1 trunk . . . 50
endpoint devices . . . 43
Ethernet WAN link . . . 53
external router . . . 53
IP telephone to gateway . . . 44
ISDN trunk . . . 50
modem after running GIW . . . 141
over-voltage protection devices . . . 52
power to the gateway . . . 41
safety ground . . . 40
Services port to computer . . . 43
sneak-current protection devices . . . 52
switch or network data port . . . 43
telephone . . . 67
trunk . . . 69
USB modem
gateway with S8300 . . . 58
in GIW . . . 141
Connections
adjunct power . . . 143
end-to-end . . . 144
Connectivity
testing after installation . . . 63
Contact closure
implementing . . . 116
installing . . . 54
port description . . . 116
Contents of gateway package . . . 23
copy ftp EW_archive CLI command . . . 88
copy ftp module CLI command . . . 88
copy ftp phone-image CLI command . . . 100
copy ftp phone-script CLI command . . . 100
copy ftp SW_imageA CLI command . . . 89
copy ftp SW_imageB CLI command . . . 89
copy running-config startup-config CLI command . . . 100
copy scp phone-script CLI command . . . 100
copy tftp EW_archive CLI command . . . 89
copy tftp module CLI command . . . 89
copy tftp phone-image CLI command . . . 100
copy tftp phone-script CLI command . . . 100
copy tftp SW_imageA CLI command . . . 89
copy tftp SW_imageB CLI command . . . 89
copy usb EW_archive CLI command . . . 94
copy usb module CLI command . . . 94
copy usb phone-image CLI command . . . 100
copy usb phone-script CLI command . . . 100
copy usb SW_imageA CLI command . . . 94
copy usb SW_imageB CLI command . . . 94
Coupled Bonding Conductor
see CBC

D

DCP
media modules, ports for in-building use only . . . 53
telephone, connecting . . . 48
Device Manager, upgrading Java applet via a USB device 94
Devices
connecting endpoint . . . 43
data and voice, connecting . . . 43
new, replacing and adding . . . 67
Dimensions of plywood board for mounting gateway . . . 17
Documentation, planning . . . 17
Downloading
CM
authentication file . . . 19
license file . . . 19
gateway
firmware to local PC . . . 94
firmware to local TFTP sever . . . 91
IP telephone
configuration files . . . 98
latest version of guide from website . . . 11
recent firmware updates . . . 21
upgrade software from CD-ROM . . . 59

E

E1 trunk, connecting . . . 50
Electronic Preinstallation Worksheet (EPW)
importing in GIW . . . 138
obtaining . . . 21
EM200
package inventory . . . 23
Emergency Transfer
see ETR
Enabling
ASG authentication in GIW . . . 56, 141
CHAP authentication . . . 56, 141
modem
gateway without S8300 . . . 55
general description . . . 55
USB
gateway with S8300 . . . 58
gateway without S8300 . . . 55
Endpoint devices
connecting . . . 43

new, replacing and adding . . . 67
Environmental conditions
mounting solution for harsh . . . 25
verifying for installation . . . 22
EPW
see Electronic Preinstallation Worksheet (EPW)
Equipment
required for installation
gathering . . . 17
removing . . . 66
unpacking . . . 24
erase phone-image CLI command . . . 101
ETH LAN port
connecting
external router to . . . 53
description . . . 116
for network switching . . . 43
ETH WAN port
connecting
Ethernet WAN link to . . . 53
external router to . . . 53
description . . . 116
Ethernet
WAN link, connecting . . . 53
ETR . . . 123
External
endpoint devices, connecting . . . 43
router, connecting to gateway . . . 53

F

Fastening chassis to wall or rack . . . 25
Feet, affixing to stand gateway on table . . . 29
Field replaceable units
adding and removing . . . 73
VoIP module . . . 73
Firmware
banks . . . 117
copying files to S8300 Server . . . 93
default bank . . . 117
downloading recent updates . . . 21
files
upgrading IP phone . . . 97
installing from TFTP server on the S8300 Server . . . 92
loading . . . 117
upgrading
example using FTP/TFTP . . . 89
gateway
CLI commands for, via FTP/TFTP . . . 88
downloading to local PC . . . 94
downloading to local TFTP server . . . 91
from primary controller . . . 85
in GIW . . . 86
in IW . . . 86
overview . . . 85
using CLI via FTP/TFTP . . . 88
using CLI via USB device . . . 93
installation worksheets, preparing . . . 89
Server Values worksheets, preparing . . . 90
with Avaya Software Update Manager . . . 85
Front panel . . . 32
gateway
buttons
ASB . . . 117
RST . . . 117
description . . . 113
media module slots . . . 114
overview . . . 113
ports
CCA . . . 116
Compact flash . . . 115
ETH WAN . . . 116
router . . . 116
Services . . . 115
USB . . . 115
system LEDs . . . 114
media modules
MM710B
LEDs . . . 118
overview . . . 117
ports . . . 118
MM711
LEDs . . . 119
overview . . . 119
ports . . . 119
MM712
LEDs . . . 120
overview . . . 120
ports . . . 120
MM714
LEDs . . . 121
overview . . . 121
ports . . . 121
MM714B
LEDs . . . 122
overview . . . 122
ports . . . 122
MM716
LEDs . . . 125
overview . . . 123
ports . . . 124
MM717
LEDs . . . 127
overview . . . 125
ports . . . 126
MM720
LEDs . . . 128
overview . . . 128
ports . . . 128
MM722

LEDs . . . 129
overview . . . 129
ports . . . 129

G

G430 cover
removing . . . 73
replacing . . . 77
Gateway
backing up to USB mass storage device . . . 107
call center . . . 145
announcements . . . 145
components, initializing in GIW . . . 138
configuration . . . 61
initial gateway in GIW . . . 137
initial in IW . . . 135
connecting
power to . . . 41
firmware
banks . . . 117
downloading files
to local PC . . . 94
to local TFTP server . . . 91
installing from TFTP server on S8300 Server . . . 92
upgrading
CLI commands for, via FTP/TFTP . . . 88
CLI commands for, via USB device . . . 94
from primary controller . . . 85
in GIW . . . 86
in IW . . . 86
overview . . . 85
using CLI via FTP/TFTP . . . 88
using CLI via USB device . . . 93
with Avaya Software Update Manager . . . 85
front panel
buttons
ASB . . . 117
RST . . . 117
description . . . 113
media module slots . . . 114
ports
CCA . . . 116
Compact flash . . . 115
ETH WAN . . . 116
router . . . 116
Services . . . 115
USB . . . 115
system LEDs . . . 114
ground block for multiple . . . 38
installation
chassis
media modules, before inserting . . . 30, 31
mounting options . . . 25
overview . . . 25
rack mounting . . . 25
tabletop installation . . . 29
wall mounting . . . 28, 29
equipment required . . . 17
non-S8300, prerequisites for . . . 18
S8300 Server, prerequisites for . . . 17
session, initializing in GIW . . . 138
mounting hardware required . . . 17
package, contents of . . . 23
prerequisites for installing S8300 Server in . . . 17
replicating to USB mass storage device . . . 107
restoring from USB mass storage device . . . 107
serial number . . . 18
specifications, technical . . . 131
supported modems . . . 18
telephone
adding to . . . 67
configuring on . . . 68
troubleshooting . . . 109
trunk
adding to . . . 68
configuring on . . . 69
USB mass storage device
backing up to . . . 107
replicating to . . . 107
restoring from . . . 107
voice modules, adding to . . . 67
Gateway Installation Wizard (GIW)
ASG authentication, enabling . . . 56, 141
authentication file, installing . . . 140
basic configuration . . . 137
CHAP authentication, enabling . . . 141
configuration, initial gateway . . . 137
description . . . 61
Electronic PreInstallation Worksheet, importing . . . 138
gateway
components, initializing . . . 138
firmware, upgrading . . . 86
installation session, initializing . . . 138
IP phone upgrade files, uploading . . . 140
modem
connecting after running GIW . . . 141
testing after running GIW . . . 142
USB
connecting . . . 141
enabling (gateway with S8300) . . . 58
enabling (gateway without S8300) . . . 55
Primary Management Interface (PMI), configuring . . . 139
running . . . 137
SNMP
V1 community strings, configuring . . . 139
V3 user, configuring . . . 139
Gigabit Ethernet port, for network switching . . . 43
Ground block for multiple gateways . . . 38
Ground conductors, attaching . . . 40
general requirements . . . 37

location . . . 37
overview . . . 37
safety ground . . . 40
Grounding
approved . . . 38
requirements . . . 37
Supplementary Ground Conductor . . . 37
verifying . . . 22
wires, attaching . . . 40
Guide
downloading latest version from website . . . 11
related resources . . . 13
safety labels . . . 11
security alert labels . . . 11
sending comments about . . . 15
trademarks . . . 14
typographical conventions . . . 11
Guides for cables . . . 25, 26

H

Help
resources for technical assistance . . . 14
technical assistance
international . . . 14
within the US . . . 14
Hot-swapping media modules . . . 67

I

ICC- VLAN
configuring using CLI . . . 150
INADS
address . . . 20
Inserting
media modules . . . 35
S8300 Server module . . . 33
Installation
after . . . 63
Avaya Partner Contact Closure Adjunct . . . 54
before you start . . . 17
CBC . . . 54
conditions good for . . . 22
contact closure . . . 54
equipment, removing . . . 66
firmware from TFTP server on the S8300 Server . . . 92
required equipment . . . 17
testing
connectivity . . . 63
LSP failover . . . 64
telephones . . . 63
trunks . . . 63
worksheets, preparing . . . 89
Installing the gateway chassis
see Gateway chassis installation
Inventory of packed items . . . 23
IP address
RAS, obtaining . . . 20
IP telephones
connecting to gateway . . . 44
not supported by local TFTP server . . . 98
supported by local TFTP server . . . 97
TFTP server upgrade example . . . 101
upgrade files
downloading . . . 98
uploading in GIW . . . 140
upgrading . . . 99
configuration files, overview . . . 97
considerations . . . 105
examples of
4602 after file stored in NVRAM . . . 103
4602SW and 4602D . . . 101
firmware files, overview . . . 97
troubleshooting . . . 104
ip tftp-server file-system size CLI command . . . 100
ISDN
BRI stations, connecting . . . 44
trunk, connecting . . . 50

L

Labels
safety . . . 11
security alert . . . 11
LAN
port
connecting IP phone to . . . 44
connecting switch to . . . 43
switch, connecting to the gateway . . . 43
LEDs
media modules
MM710B . . . 118
MM711 . . . 119
MM712 . . . 120
MM714 . . . 121
MM714B . . . 122
MM716 . . . 125
MM717 . . . 127
MM720 . . . 128
MM722 . . . 129
system . . . 114
License file
for CM
obtaining . . . 19
required for LSP . . . 19
Lightning exposure . . . 53
Limitations
media module combinations . . . 31
LINE port, connecting analog telephone to . . . 46
LSP

Avaya Aura Communication Manager version requirements . . . 19
failover testing . . . 64
license file requirements . . . 19

M

Media Gateway installation
before inserting media modules . . . 31
connecting
endpoint devices . . . 43
power to . . . 41
ground conductors
attaching . . . 37
location . . . 37
installing
chassis . . . 25
media modules . . . 30
order of installation . . . 25
Restricted Access Location . . . 38
S8300 server module, inserting . . . 33
safety ground, connecting . . . 40
Media module slots . . . 114
Media modules
before installing . . . 31
capacity . . . 31
combination limitations of . . . 31
firmware
upgrading via FTP/TFTP . . . 88
upgrading via USB device . . . 94
for indoor use only . . . 49
gateway chassis, inserting into . . . 35
hot-swapping . . . 67
installing . . . 30
MM710B . . . 117
MM711 . . . 119
MM712 . . . 120
MM714 . . . 121
MM714B . . . 122
MM716 . . . 123
MM717 . . . 125
MM720 . . . 128
MM722 . . . 129
new, replacing and adding . . . 67
slot allocation . . . 31
slots, permitted . . . 31
voice modules, adding . . . 67
Messaging
Avaya Aura Communication Manager . . . 145
MM710 and MM170B
media module
circuit protection devices for outdoor endpoints 52
MM710 and MM710B
E1/T1 port, connecting E1/T1 trunk to . . . 50
MM710B
media module
description . . . 117
LEDs . . . 118
ports . . . 118
MM711
analog port
connecting analog telephone to . . . 46
connecting analog trunk to . . . 49
media module
circuit protection devices for outdoor endpoints . 52
description . . . 119
LEDs . . . 119
ports . . . 119
MM712
DCP ports
connecting DCP phones to . . . 48
for in-building use only . . . 53
media module
description . . . 120
LEDs . . . 120
ports . . . 120
MM714
analog trunk ports, connecting analog trunks to . . . 49
LINE port, connecting analog telephone to . . . 46
media module
description . . . 121
LEDs . . . 121
ports . . . 121
MM714B
media module
description . . . 122
LEDs . . . 122
ports . . . 122
MM716
analog port
connecting analog telephone to . . . 46
connecting analog trunk to . . . 49
attaching amphenol cable to . . . 51
media module
connecting to punch down block for RJ-45 or RJ-11 jacks . . . 51
description . . . 123
LEDs . . . 125
ports . . . 124
MM717
attaching amphenol cable to . . . 51
DCP ports
connecting DCP phones to . . . 48
for in-building use only . . . 53
media module
connecting to punch down block for RJ-45 or RJ-11 jacks . . . 51
description . . . 125
LEDs . . . 127
ports . . . 126
MM720

ISDN ports, connecting ISDN BRI trunks to 50
media module
connecting ISDN BRI stations to 44
description 128
LEDs 128
ports 128
MM722
ISDN ports, connecting ISDN BRI trunks to 50
media module
description 129
LEDs 129
ports 129
Modem
connecting
after running GIW 141
for remote access 55
gateway without S8300 55
USB
gateway with S8300 58
gateway without S8300 55
USB in GIW 141
dial backup 55
enabling
for remote access 55
gateway without S8300 55
USB in GIW
gateway with S8300 58
gateway without S8300 55
permanent connection for reporting alarms 55
settings, Configure Server Maintenance Web page 57
supported by gateway 18
testing connection
after running GIW 142
gateway with S8300 59
gateway without S8300 57
USB
supported by gateway 133
supported by S8300 133
Mounting
brackets
for wall 28
attaching to gateway 28
gateway
in 19-inch rack 25
in rack 27
on tabletop 29
on wall 28, 29
hardware required 17
options for chassis 25
mounting brackets for rack
attaching 27
checks before 27
types of 25
with cable guides 26
without cable guides 26
Multi-Tech modem
MT5634ZBA-USB 55
Mutual inductance coupling 53

N

Network
data port, connecting to gateway 43
NVRAM
initializing with a jumper 110

O

Ordering
analog trunk 69
trunk 69
Outdoor installation 52
Out-of-building installation 52
Over-voltage protection 52

P

Package inventory 23
Password
RAS, obtaining 20
PC
downloading gateway firmware to local 94
Physical description 32
Physical description of gateway front panel 113
Planning
documentation 17
installation 17
Platform, hardware, for harsh environment 25
Plugging in
endpoint devices 43
the gateway 41
Plywood board
dimensions 17
using to wall-mount gateway 29
Ports
CCA 116
connecting
data and voice devices to 43
endpoint devices to 43
contact closure 116
ETH LAN 116
ETH WAN 116
MM710B 118
MM711 119
MM712 120
MM714 121
MM714B 122
MM716 124
MM717 126

MM720 . . . 128
MM722 . . . 129
router . . . 116
Services . . . 115
switch . . . 116
switch or network data, connecting . . . 43
USB . . . 115
Positioning
gateway in rack . . . 27
S8300 media module . . . 33
Power
connection
adjunct . . . 143
end-to-end . . . 144
to gateway . . . 41
cords
obtaining . . . 133
specifications . . . 133
outlets, checking available number of . . . 22
verification . . . 22
Pre-installation activities . . . 17
Preinstallation worksheet
see Electronic Preinstallation Worksheet (EPW)
Preparation
installation worksheets . . . 89
Server Values worksheets . . . 90
telephone configuration . . . 68
trunk configuration . . . 69
Primary controller
upgrading gateway firmware from . . . 85
Primary Management Interface (PMI)
configuring in GIW . . . 139
configuring using CLI . . . 150

R

Rack mounting
brackets . . . 25
the gateway chassis . . . 25
RAM card
replacing . . . 79
upgrading . . . 79
RAS
IP address
entering in GIW . . . 56
obtaining . . . 20
password, obtaining . . . 20
Remote
access, enabling . . . 55
Removing installation equipment . . . 66
Replacing
endpoint devices . . . 67
Replicating the gateway to USB mass storage device 107
Required
equipment . . . 17
Reset button . . . 117
reset CLI command . . . 100
Restoring the gateway from USB mass storage device 107
Restricted Access Location . . . 38
RFA access . . . 18
RJ-45 splitter for connecting two BRI stations . . . 45
Router
connecting external to gateway . . . 53
ports . . . 116
RST button . . . 117
Rubber feet, affixing to stand gateway on table . . . 29
Ruggedized mounting solution for harsh environment . 25
Running Gateway Installation Wizard (GIW) . . . 137

S

S8300
Server
call center solution . . . 145
connecting to USB modem . . . 58
copying firmware to . . . 93
gateway chassis, inserting into . . . 33
installing firmware from the TFTP server on . . 92
prerequisites for installing in gateway . . . 17
Safety
ground, connecting . . . 40
labels . . . 11
save translation lsp CLI command . . . 65
Screws required for mounting gateway . . . 17
Securing amphenol cable to MM716 or MM717 . . . 51
Security alert labels . . . 11
Serial number of gateway . . . 18
Server Values worksheets, preparing . . . 90
Services
port . . . 115
connecting a computer to . . . 43
show application-memory CLI command . . . 100
Single Sign-On (SSO) . . . 18
Site
conditions, checking before installation . . . 22
requirements . . . 22
Sneak-current protection . . . 52
SNMP
V1 community strings, configuring in GIW . . . 139
V3 user, configuring in GIW . . . 139
Software
configuration . . . 61
recording telephone information for . . . 68
recording trunk information for . . . 70
software
upgrading
in IW . . . 86
Software Update Manager . . . 85
Specifications, technical . . . 131
power cord . . . 133

Supplementary Ground Conductor 37
if ground block is used 40
if ground block not used 40
Switch
connecting to gateway 43
port 116

T

T1
trunk, connecting 50
Tabletop installation of the gateway chassis 29
Technical assistance
international 14
resources 14
within the US 14
Technical specifications 131
power cord 133
Telephone
adding to gateway 67
configuring 68
connecting 67
IP, connecting to gateway 44
software configuration, recording information for . 68
testing 68
after installation 63
troubleshooting
one 109
Terminating telephones on the MM717 and MM716 . 51
Testing
installation
connectivity 63
LSP failover 64
overview 63
telephones 63
trunks 63
modem connection
gateway with S8300 59
gateway without S8300 57
telephone 68
trunk 70
WAN link 71
TFTP server
downloading gateway firmware to local 91
for upgrading IP phones 97
installing firmware from, on the S8300 Server . . . 92
IP telephones
not supported by local 98
supported by local 97
upgrade example 101
setting up
overview 91
uploading IP phone upgrade files
in GIW 140
Trademarks 14
Troubleshooting
CLI not accessible 110
gateway has no power 109
IP telephone upgrades 104
overview 109
telephone
one stops working 109
Trunk
adding
to gateway 68
analog
connecting to TRUNK port 49
ordering 69
configuring
on gateway 69
connecting 69
ordering 69
software configuration, recording information for . . 70
testing 70
after installation 63
TRUNK port, connecting analog trunk to 49

U

Unpacking 24
Upgrade memory kit
installing 79
replacing the RAM card 79
Upgrading
firmware
example
using a USB device 94
using FTP/TFTP 89
installation worksheets, preparing 89
Server Values worksheets, preparing 90
gateway firmware
CLI commands for, via FTP/TFTP 88
downloading
to local PC 94
to local TFTP server 91
from primary controller 85
in GIW 86
in IW 86
overview 85
using CLI
via USB device 93
using CLI via FTP/TFTP 88
with Avaya Software Update Manager 85
IP telephones 99
configuration files
downloading 98
overview 97
considerations 105
examples of
4602 after file stored in NVRAM 103

4602SW and 4602D 101
firmware files, overview 97
troubleshooting 104
media modules and devices 67
USB
mass storage device
backing up the gateway 107
CLI commands for upgrading firmware 94
example of upgrading firmware 94
replicating the gateway 107
restoring the gateway 107
upgrading gateway firmware using CLI 93
modem
connecting in GIW 141
gateway with S8300 58
gateway without S8300 55
enabling in GIW
gateway with S8300 58
gateway without S8300 55
supported by gateway 55
port 115
USB Modem
supported by gateway 133
supported by S8300 133

V

Verifying
environmental conditions before installation . . . 22
grounding 22
power 22
VoIP module
field replaceable 73
inserting 75
removing 77

W

Wall mounting
brackets 28
the gateway chassis 28, 29
WAN
configuring on gateway 71
connecting 53
link
connecting 53
ordering 70
preparing for configuration 71
testing 71
Worksheets
installation, preparing 89
Server Values, preparing 90