



Deploying and Upgrading Avaya G430 Branch Gateway

Release 10.2.x
Issue 2
March 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Documentation disclaimer

"Documentation" means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

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

Copyright

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

written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

How to Get Help

For additional support telephone numbers, go to the Avaya Support website: <http://www.avaya.com/support>. If you are:

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Product Safety Standards

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

- IEC 62368-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 62368-1 / UL 62368-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaitte
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC)

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

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

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

For a Class B digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to

try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
 - answered by the called station,
 - answered by the attendant,
 - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
 - routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

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

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

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

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

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1K N	6.0F	RJ48C, RJ48M
	04DU9.1S N	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

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

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

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

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 5 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is

designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

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

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

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

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

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available by contacting Avaya Support website at: <https://support.avaya.com>.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

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

This product meets the applicable Industry Canada technical specifications/Le présent matériel est conforme aux spécifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity



This device when installed complies with the essential requirements and other relevant provisions of the EMC Directive 2014/30/EU, and Safety LV Directive 2014/35/EU.

A copy of the Declaration may be obtained from <https://support.avaya.com> or Avaya LLC, 350 Mt. Kemble Avenue, Morristown, NJ USA 07960 USA.

European Union Battery Directive



Avaya LLC supports European Union Battery Directive 2006/66/EC. Certain Avaya LLC products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage

could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

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

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

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction	12
Purpose	12
Change history	12
Chapter 2: Planning and pre-configuration	13
Installation equipment	13
Mounting equipment	13
Installation hardware	13
Obtaining the Branch Gateway serial number	14
Downloading software from PLDS	14
License file with Survivable Remote Server	15
Assigning license and authentication files	15
Downloading the firmware	15
Branch Gateway authentication file	16
S8300 upgrade with Solution Deployment Manager	16
Site requirements	16
Temperature and clearance verification	16
Power outlet verification	17
Grounding requirements	17
Firmware specifications	17
Unpacking and checking package contents	24
Branch Gateway package contents	25
EM200 package contents	25
Chapter 3: Branch Gateway and EM200 installation	26
Branch Gateway chassis mounting	26
Attaching a mounting bracket to the Branch Gateway	26
Brackets without cable guides	27
Brackets with cable guides	27
Mounting Branch Gateway in the rack	28
Placing Branch Gateway on a table	28
Wall mounting requirements	28
Mounting the Branch Gateway on a wall	29
Installing the EM200 expansion modules	30
Media module installation	30
Limitations of media module combinations	31
Slot allocation	31
Media module installation precautions	33
Installing S8300 Server	33
Installing media modules	34
General grounding requirements	34

Installation location.....	35
Supplementary ground conductor.....	35
Ground block.....	35
Restricted access location (RAL).....	36
Approved grounds.....	36
NFPA 70: NEC.....	36
ANSI/EIA/TIA-607.....	38
Safety ground connections.....	39
Attaching the ground wires.....	39
Attaching ground wires to purchased ground blocks.....	40
Attaching ground wires without ground blocks.....	40
Connecting the EM200 expansion module to a power source.....	40
Connecting Branch Gateway to a power source.....	41
Chapter 4: Connecting peripheral devices.....	42
Data and voice device connections.....	42
Switch and network data ports.....	42
IP phone connections.....	42
Connecting a phone to Branch Gateway.....	43
ISDN BRI station connections.....	43
Connecting an ISDN BRI station to an ISDN port.....	43
Connecting two ISDN BRI stations to an ISDN port.....	43
Connecting an analog phone.....	44
Connecting a DCP phone to an MM712 or MM717 media module.....	45
Connecting an analog trunk.....	46
Connecting an analog DID trunk.....	46
Connecting an E1/T1 trunk.....	47
Connecting an ISDN BRI trunk.....	47
Connecting phones to MM716 and MM717 media modules.....	48
Connecting an MM716 and MM717 front panel connector to a punch-down block.....	48
Circuit protection installation.....	49
Coupled Bonding Conductor installations.....	50
Installing the CBC.....	50
Avaya Partner Contact Closure Adjunct installations.....	51
Installing the contact closure.....	51
Chapter 5: Connecting and enabling a USB modem for remote access.....	52
Modems for remote access.....	52
Chapter 6: Branch Gateway configuration.....	53
Configuring basic Branch Gateway connectivity.....	53
Chapter 7: Post-installation verification.....	56
Roadmap for post installation.....	56
Installation testing.....	56
Testing data connectivity.....	56
Testing telephones.....	56

Testing trunks.....	57
Testing LSP failover.....	57
IP addresses and controllers.....	58
Removing the installation equipment.....	58
Chapter 8: Media module and device additions.....	59
Media module additions.....	59
Voice module additions.....	59
Telephone additions.....	59
Telephone connections.....	60
Configuration of telephones on Communication Manager.....	60
Telephone information recordings for software configuration.....	60
Testing the telephone.....	60
Trunk additions.....	61
Trunk ordering.....	61
Special considerations when ordering an analog trunk.....	61
Connecting the trunk.....	61
Trunk configurations on Communication Manager.....	61
Trunk information recordings for software configuration.....	62
Testing the trunk.....	62
Broadband line additions.....	62
Broadband line ordering.....	62
Broadband line connections.....	62
Broadband line configuration.....	62
Testing the Broadband link.....	63
Avaya Partner Contact Closure Adjunct additions.....	63
Chapter 9: Field Replaceable Unit upgrades and replacements.....	64
Inserting or removing an MP10, MP20, MP80, or MP120 VoIP module.....	64
Removing the G430 cover.....	65
Inserting a VoIP module.....	66
Removing a VoIP module.....	68
Replacing the G430 cover.....	69
Installation of the upgrade memory kit.....	70
The upgrade memory kit.....	70
RAM card replacement.....	71
Compact flash memory cards.....	72
Inserting a compact flash memory card.....	72
Compact flash memory card removals.....	74
Swapping compact flash memory cards.....	74
Replacing a compact flash memory card while retaining the current announcements.....	74
Downgrading from a compact flash to internal flash memory.....	75
Chapter 10: Branch Gateway firmware upgrade.....	77
Firmware upgrades using Solution Deployment Manager.....	78
Upgrading firmware using the command line interface through SCP/FTP/TFTP/HTTPS.....	78

CLI commands for upgrading Branch Gateway firmware via SCP/FTP/TFTP/HTTPS.....	79
Example upgrade via SCP/FTP/TFTP/HTTPS using the CLI.....	80
Installation worksheets.....	80
Server Values worksheet.....	80
File server setup.....	81
Downloading Branch Gateway firmware files to a local file server.....	81
Sample software and firmware file names.....	82
Example failure message if the wrong image is used.....	83
Checking the G430 hardware vintage from the Branch Gateway CLI.....	83
Checking the G430 hardware vintage from the Communication Manager web interface.....	84
Upgrading Branch Gateway firmware using the CLI via a USB device.....	85
CLI commands for upgrading Branch Gateway firmware via a USB device.....	86
Example upgrade using the CLI via a USB device.....	86
Downloading firmware files to a local computer.....	86
Chapter 11: Upgrading IP phone configuration and firmware files.....	88
IP phone configuration and firmware file upgrades.....	88
IP phones supported by the local TFTP server feature.....	88
CLI commands for upgrading Branch Gateway firmware via SCP.....	89
Administering the upgrade.....	90
Upgrade administration.....	90
TFTP IP telephone upgrade examples.....	92
Upgrading 4602SW and 4602D phones.....	92
Upgrading 4620 IP phones.....	94
Failure scenarios and repair actions.....	95
Upgrading considerations.....	96
Chapter 12: Branch Gateway backups and restores.....	97
Best practices for backup.....	97
Backup and restore operations.....	98
Backing up G430 gateway.....	98
Restoring a gateway backup.....	99
Preserving SNMP engine ID.....	100
Backup and restore for G430 gateway replacement.....	101
Backing up and restoring for non-FIPS mode gateways.....	101
Backing up and restoring for FIPS mode gateways.....	103
Gateway replacement checklist.....	104
Non-FIPS mode gateway replacement checklist.....	104
FIPS mode gateway replacement checklist.....	106
Post restoration of gateway checks.....	107
Chapter 13: Troubleshooting.....	108
One telephone stops working.....	108
Identifying the problem when one phone stops working.....	108
Proposed Solution.....	108
No power on the Branch Gateway.....	108

Proposed Solution.....	108
CLI is not accessible.....	109
NVRAM Init.....	109
Proposed Solution.....	109
Chapter 14: Front panel description.....	113
The front panel of the Branch Gateway chassis without media modules.....	113
Media module slots.....	114
System (SYSTM) LEDs.....	114
USB ports.....	115
Console port (Console/CNSL).....	115
Services port (Services/SVCS).....	115
Compact Flash (CMPCT FLSH) Interface.....	115
The Emergency Transfer Relay (ETR) port.....	116
Contact Closure (CCA) port.....	116
Implementing the Contact Closure feature.....	116
Router port (ETH WAN).....	116
Switch ports (ETH LAN).....	116
RST and ASB buttons.....	116
Loading firmware from a bank other than the default bank during startup.....	117
The front panel of the Avaya MM710B media module.....	117
MM710B ports.....	117
MM710B LEDs.....	118
The front panel of the Avaya MM711 media module.....	118
MM711 ports.....	118
MM711 LEDs.....	119
The front panel of the Avaya MM712 media module.....	119
MM712 ports.....	119
MM712 LEDs.....	119
The front panel of the Avaya MM714 media module.....	120
MM714 ports.....	120
MM714 LEDs.....	120
The front panel of the Avaya MM714B media module.....	120
MM714B ports.....	121
MM714B LEDs.....	121
The front panel of the Avaya MM716 media module.....	121
MM716 ports.....	122
MM716 LEDs.....	123
The front panel of the Avaya MM717 media module.....	123
MM717 ports.....	123
MM717 LEDs.....	124
The front panel of the Avaya MM720 media module.....	125
MM720 ports.....	125
MM720 LEDs.....	125

Front panel of the MM721 media module.....	125
MM721 media module ports.....	125
MM721 media module LEDs.....	126
The front panel of the Avaya MM722 media module.....	126
MM722 ports.....	126
MM722 LEDs.....	126
Chapter 15: Technical specifications.....	127
Specifications.....	127
EM200 specifications.....	128
Power cord specifications.....	128
USB modems supported by the Branch Gateway.....	129
USB modems supported by the S8300.....	129
Chapter 16: Power supplies and adjunct systems.....	130
Typical adjunct power connections.....	130
Typical adjunct power connections end-to-end.....	131
Avaya Aura® Communication Manager Messaging application.....	132
Call Center.....	132
About Avaya Branch Gateway announcement software.....	132
Chapter 17: Information checklists.....	133
Installation checklist.....	133
Serial number and login information.....	134
Logins.....	134
Quick setup for Branch Gateway Processor (MGP).....	134
Installation site information.....	136
Chapter 18: Equipment list.....	137
Chapter 19: Resources.....	142
Branch Gateway documentation.....	142
Finding documents on the Avaya Support website.....	142
Accessing the port matrix document.....	143
Avaya Documentation Center navigation.....	143
Training.....	144
Viewing Avaya Mentor videos.....	145
Support.....	145

Chapter 1: Introduction

Purpose

This document contains Branch Gateway installation, configuration, upgrading, basic maintenance checklist, and procedures.

This document is intended for system administrators, implementation, and support personnel.

Change history

Issue	Release Date	Summary of changes
2	March 2026	Updated the following section: • Branch Gateway backups and restores on page 97 Added the following sections: • Best practices for backup on page 97. • Backup and restore operations on page 98. • Backing up G430 gateway on page 98. • Restoring a gateway backup on page 99. • Preserving SNMP engine ID on page 100. • Backup and restore for G430 gateway replacement on page 101. • Backing up and restoring for non-FIPS mode gateways on page 101. • Backing up and restoring for FIPS mode gateways on page 103. • Non-FIPS mode gateway replacement checklist on page 104. • FIPS mode gateway replacement checklist on page 106. • Post restoration of gateway checks on page 107.
1	December 2023	Release 10.2.x document.

Chapter 2: Planning and pre-configuration

Before installing Branch Gateway, you must read the planning documentation and prepare equipment required for installation.

Installation equipment

Ensure you have the following equipment before installing Branch Gateway:

- One loop start analog trunk for connecting a laptop for configuration.
- A separate phone line for communication during remote configuration.

Mounting equipment

Ensure you have the following equipment before mounting Branch Gateway:

- A crosspoint screwdriver for rack mounting or wall mounting.
- For mounting on a flat wall, screws to fasten Branch Gateway to the wall.
- For mounting on a non-flat wall:
 - A 48 in. x 48 in. (1.2 m x 1.2 m) plywood board (US 3/4 in. plywood), 0.75 in. (20 mm) thick.
 - Wood screws to fasten Branch Gateway to the plywood board.
 - Screws to fasten the plywood board to the wall (10-12 pan head screws of at least 3/4 in.).

Installation hardware

If you install an S8300 server, ensure that you have the following hardware:

- One USB CD/DVD-ROM drive (Avaya Comcode 700406267).
- A laptop computer with Internet Explorer.

If you do not install an S8300 server, ensure that you have the following hardware:

- A PC on the local network.
- Optional USB flash drive.
- If using the serial port, the port being used will appear under a list in Device Manager on your laptop.

Related links

[USB modems supported by the Branch Gateway](#) on page 129

Obtaining the Branch Gateway serial number

About this task

You need to obtain the Branch Gateway serial number to add the Gateway in Communication Manager. The serial number can be found by running the `show system` command.

Procedure

View the serial number label on the back of the Branch Gateway chassis.

Downloading software from PLDS

Procedure

1. On your web browser, type <http://plds.avaya.com> to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS Home page, select **Assets**.
4. Click **View Downloads**.
5. Click the search icon  for Company Name.
6. In the Search Companies dialog box, do the following:
 - a. In the **%Name** field, type `Avaya` or the Partner company name.
 - b. Click **Search Companies**.
 - c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
 - In **Download Pub ID**, type the download pub ID.
 - In the **Application** field, click the application name.
8. Click **Search Downloads**.

9. In the **Download Manager** box, click the appropriate **Download** link.

 Note:

The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.

10. If you use the Download Manager, click **Details** to view the download progress.
11. Select a location where you want to save the file, and click **Save**.
12. **(Optional)** When the system displays the security warning, click **Install**.

When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

License file with Survivable Remote Server

If you are installing an S8300 server as a Survivable Remote Server (SRS), the license file for S8300 must have Communication Manager release that is equal to or later than that of the server that acts as a primary controller. In this case, if control passes to the SRS, it can have the same level of call processing as the primary controller.

The SRS must have a version of Avaya Aura[®] Communication Manager, which is the same as the primary controller version.

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

Assigning license and authentication files

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

You can use the Maintenance Web Interface to assign the IP address of the WebLM Server.

Downloading the firmware

About this task

You need to download the latest version of firmware for Branch Gateway and media modules to your laptop.

Procedure

1. Go to the [Avaya support](#) site.
2. Select the latest version of the firmware image file for the hardware you are installing.
3. Download the required firmware image file.
4. Download the Communication Manager service pack that is required for the upgrade.

Branch Gateway authentication file

An authentication file is preinstalled in Branch Gateway. You can update it if needed. Check the authentication file version using the `show auth-file info` function. Branch Gateway firmware versions 6.x and 7.0.0 use 6.x authentication files.

Branch Gateway authentication file is not used in Release 7.1.2 and later.

When FIPS mode is enabled, you cannot log in with the Services access level using the authentication file.

S8300 upgrade with Solution Deployment Manager

From Release 7.0, you can upgrade S8300 using Solution Deployment Manager. For more information about upgrading S8300 firmware using Solution Deployment Manager, see *Administering Avaya Aura® System Manager*.

Site requirements

Inspect the site before installing Branch Gateway. Ensure that the environmental conditions, power and grounding availability, safety, and security conditions meet the Branch Gateway installation requirements.

If the site conditions do not meet the requirements, contact your project manager before proceeding with the installation.

Temperature and clearance verification

Verify that temperatures and clearances are within the recommended range. You can install the Branch Gateway in a 19-inch rack, mount on a wall, or place on a sturdy table. The ambient temperature must be in the range of 32 to 104°F (0 to 40°C). The humidity must not be higher than 90%. If the conditions are beyond the recommended limits, the thermal sensors can shut down the equipment and it can be damaged.

Related links

[Specifications](#) on page 127

Power outlet verification

You must ensure that the required number of power outlets is available. Verify that Branch Gateway and other equipment in the rack do not overload the branch circuit and power distribution strip.

Related links

[Power cord specifications](#) on page 128

Grounding requirements

Ensure that the installation site has access to approved grounds. A trained technician or a licensed electrician must verify all grounds and install the supplementary ground conductor.

AC powered Branch Gateway has multiple ground connections. The AC power cords contain ground conductors and must be connected to AC outlets that have earth contacts. The supplementary ground conductor provides a non-removable ground even when the AC cords are disconnected.

In Finland, Norway, and Sweden, Branch Gateway must be installed in a restricted access location (RAL). If you have any questions about the safety conditions, contact your project manager.

Related links

[Restricted access location \(RAL\)](#) on page 36

Firmware specifications

New Comcode numbers for G430 Branch Gateway

Old codes are active for G430 Branch Gateway with the imbedded MP20 and MP80 bundle option.

- 700503274 : G430 120 channel DSP daughter board – Single MP120 for upgrades
- 700506957 : G430 MP120 Media Gateway – New bundle no on board MP20 and preinstalled MP120
- 700506958 : G430 MP120 Media Gateway Non-GSA – New bundle number on board MP20 and preinstalled MP120
- 700508198 : G430 120 CHANNEL DSP daughter board
- 700512173 : G430 V3 40 CHANNEL GSA
- 700512174 : G430 V3 40 CHANNEL NON-GSA

Minimum G430 Branch Gateway firmware requirements

Firmware version	Build	v1a	v2a (MP120 Preinstalled)	v3	Comments	Recommended Communication Manager version
BGW 10.2	43.9.0	Yes	Yes	Yes		AA 10.2, CM 10.2 AA 10.1.x, CM 10.1.x AA 10.1, CM 10.1 If your Branch Gateway is running Build 38.20.0 or earlier, you must install Release 7.1.0.4 Build 38.21.2 before upgrading to Build 43.9.0.
BGW 10.1	42.4.0	Yes	Yes	Yes	-	AA 10.1, CM 10.1 AA 8.1.x, CM 8.1.x AA 8.0.x, CM 8.0.x You can upgrade to Release 10.1 from Build 42.4.0 and earlier only after installing Release 7.1.0.5 Build 38.21.3.

Table continues...

Firmware version	Build	v1a	v2a (MP120 Preinstalled)	v3	Comments	Recommended Communication Manager version
BGW 8.1	41.9.0	Yes	Yes	Yes	MP120 Support	AA 8.1, CM 8.1 AA 8.0, CM 8.0 AA 7.1.x, CM 7.1.x AA 7.0.x, CM 7.0.x + You can upgrade to Release 8.1 from Build 41.9.0 and earlier only after installing Release 7.1.0.3 Build 38.21.1.
BGW 8.0	40.10.0	Yes	Yes	Yes	MP120 Support	AA 8.0, CM 8.0 AA 7.1.x, CM 7.1.x AA 7.0.x, CM 7.0.x + AA 6.3.x, CM 6.3.x + You can upgrade to Release 8.0 from Build 40.10.0 and earlier only after installing Release 7.1.0.3 Build 38.21.1.

Table continues...

Firmware version	Build	v1a	v2a (MP120 Preinstalled)	v3	Comments	Recommended Communication Manager version
BGW 7.1.3	39.12.0	Yes	Yes	Yes	MP120 Support	AA 7.0 FP 1, CM 7.0.1 AA 7.0 FP 1, CM 7.0.1 AA 7.0, CM 7.0+ AA 6.2 FP 4, CM 6.3.6+ AA 7.1, CM 6.3.x, AA 7.0, CM 7.1.2 You can upgrade to Release 7.1.3 from Build 39.12.0 and earlier only after installing Release 7.1.0.3 Build 38.21.1.

Table continues...

Firmware version	Build	v1a	v2a (MP120 Preinstalled)	v3	Comments	Recommended Communication Manager version
BGW 7.1.2	39.x.y	Yes	Yes	No	MP120 Support	AA 7.0 FP 1, CM 7.0.1 AA 7.0 FP 1, CM 7.0.1 AA 7.0, CM 7.0+ AA 6.2 FP 4, CM 6.3.6+ AA 7.1, CM 6.3.x, AA 7.0, CM 7.1.2 You can upgrade to Release 7.1.2 from Build 39.5.0 and earlier only after installing Release 7.1.0.3 Build 38.21.1.

Table continues...

Firmware version	Build	v1a	v2a (MP120 Preinstalled)	v3	Comments	Recommended Communication Manager version
BGW 7.1.0+	38.16.0 +	Yes	Yes	No	MP120 Support	AA 7.0 FP 1, CM 7.0.1 AA 7.0 FP 1, CM 7.0.1 AA 7.0, CM 7.0+ AA 6.2 FP 4, CM 6.3.6+ AA 7.1, CM 6.3.x, AA 7.0 Branch Gateway requires a 7.x build (37+) to successfully upgrade to Build 38.8.0 or later. Earlier builds will fail with the Invalid file error type. If Branch Gateway is running 36.x or earlier build, you must upgrade to 37.x.y before upgrading to 38.x.y.
BGW 7.0.1.2	37.41.0	Yes	Yes	No	MP120 Support	AA 7.0 FP 1
BGW 7.0.1.1	37.39.0	Yes	Yes	No	MP120 Support	AA 7.0, CM 7.0
BGW 7.0.1	37.38.0 +	Yes	Yes	No	MP120 Support	AA 7.0 FP 1, CM 7.0.1 AA 7.0, CM 7.0+ AA 6.2 FP 4, CM 6.3.6+

Table continues...

Firmware version	Build	v1a	v2a (MP120 Preinstalled)	v3	Comments	Recommended Communication Manager version
BGW 7.0.0.2	37.21.0	Yes	Yes	No	MP120 Support	AA 7.0, CM 7.0 AA 6.2 FP 4 CM 6.3.6+
BGW 7.0.0.1	37.20.0	Yes	Yes	No	MP120 Support	AA 7.0, CM 7.0 AA 6.2 FP 4 CM 6.3.6+
BGW 7.0	37.20.0	Yes	Yes	No	MP120 Support	AA 7.0, CM 7.0 AA 6.2 FP 4 CM 6.3.6+
BGW 6.3.14+	36.18.0	Yes	Yes	No	MP120 Support	CM 6.3.x, AA 7.0
BGW 6.3.7 – 6.3.13	36.16.0 +	Yes	Yes	No	MP120 Support	AA 6.2 FP 4 CM 6.3.6+
BGW 6.3.6 JITC	36.x.y	Yes	Yes	No	MP120 Support	AA 6.2 FP 4 CM 6.3.6 AA 6.2 FP3 CM 6.3.2+ (CM supports all 120 channels)
BGW 6.3.5	35.x.y	Yes	Yes	No	MP120 Support V150.1 Features	AA 6.2 FP3 CM 6.3.2+ (CM supports all 120 channels)
BGW 6.3.1	34.6.0	Yes	No	No	No BGW support MP120	AA6.2 FP3 CM6.3.2 – Oct 2013 (CM supports all 120 channels)
BGW 6.3	33.13.0	Yes	No	No	No BGW support MP120	AA 6.2 FP2 CM 6.3 – May 2013 (CM supports all 120 channels)

Table continues...

Firmware version	Build	v1a	v2a (MP120 Preinstalled)	v3	Comments	Recommended Communication Manager version
BGW 6.2.1	32.26.0	Yes	No	No	No BGW support MP120	AA 6.2 FP1 CM 6.2 sp 4 – Dec 2012 (CM blocks more than 105 channels)
BGW 6.1	31.26.0	Yes	No	No	No BGW support MP120	CM 6.0.1 (CM blocks more than 105 channels)

Unpacking and checking package contents

About this task

Before installing Branch Gateway and EM200, you need to unpack and check the package contents.

Electrostatic alert:

Wear an anti-static wrist ground strap when handling components of Branch Gateway or EM200. Connect the strap to an approved ground, such as an unpainted metal surface.

Procedure

1. Unpack Branch Gateway and accessories.
2. Check the package contents against the customer order.
3. Cross-check the customer order with the planning documentation.

For the list of media modules, phones and other equipment, and their placement, see your planning and shipping documentation.

4. Verify that all necessary elements have been received and are in good condition.
5. Do a damage inspection of the assembly and its component as follows:
 - a. Examine all relevant component for damage.
 - b. Make a 'defective on arrival - DOA' report or RMA to the operator.

Do not move the shipping carton until the operator examines it. The operator or regional representative initiates the necessary procedure to process the RMA. They guide the network administrator on how to return the damaged package, if necessary.

- c. If no damage is found, unwrap all the components and dispose empty package / cartons(s) under country-specific environmental regulations.

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

Branch Gateway package contents

The Branch Gateway chassis and accessories are shipped in a box. The package contains the following items:

- 1 Branch Gateway chassis. The required media modules are installed.
- One accessories box, containing:
 - Two 19" mounting brackets
 - One cable management assembly
 - Two wall mounting brackets
 - One supplementary ground conductor
 - Nine 4-40 flat head screws
 - Four rubber feet
- Auto-run CD

The Avaya Partner Contact Closure adjunct box, if ordered, comes in a separate package.

EM200 package contents

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

- One EM200 chassis
- One accessories box that contains:
 - One expansion cord
 - Two standard mounting brackets
 - One mounting bracket with cable guides
 - One supplementary ground conductor
 - Nine 4-40 flat head screws
 - Four rubber feet

Chapter 3: Branch Gateway and EM200 installation

Branch Gateway installation includes the following steps:

No.	Task	Reference	✓
1	Install the Branch Gateway chassis.	Branch Gateway chassis mounting on page 26	
2	Install the EM200 expansion modules.	Installing the EM200 expansion module on page 30	
3	Install media modules.	Media module installation on page 30	
4	Attach ground conductors.	Safety ground connections on page 39	
5	Connect EM200 to a power source.	Connecting the EM200 expansion modules to a power source on page 40	
6	Connect Branch Gateway to a power source.	Connecting Branch Gateway to a power source on page 41	

Branch Gateway chassis mounting

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

Electrostatic alert:

When handling any components of S8300 Server or Branch Gateway, wear an antistatic wrist ground strap. Connect the strap to an approved ground, such as an unpainted metal surface.

Attaching a mounting bracket to the Branch Gateway

About this task

Branch Gateway is supported by mounting screws through two mounting ears. You should mount units in the lower positions first to avoid balancing and cabling issues.

There are two types of mounting brackets provided with the Branch Gateway:

- Without cable guides: two mounting brackets are provided.

- With cable guides: one mounting bracket is provided. This bracket provides guides for electrical cables and is useful for cable management.

Procedure

1. Place a bracket at the required mounting position.
2. Attach the bracket to the chassis with three of the nine 4-40 flat head screws provided.
3. Tighten the screws with a screwdriver.

Brackets without cable guides

You can attach mounting brackets without cable guides in either of the following positions:

- To each side of the Branch Gateway front for fastening the chassis to the rack at the front.



- To the middle of each side of the Branch Gateway panel for fastening the chassis to the rack at the middle.



Brackets with cable guides

You can attach a mounting bracket with cable guides to the front of Branch Gateway on one side. If you fasten the chassis to the rack at the front, use the mounting bracket with cable guides as a front bracket.

If you fasten the chassis to the rack at the middle, use the mounting bracket with cable guides at the chassis front together with two regular mounting brackets on chassis sides. In this case, the mounting bracket with cable guides serves for cable management only: You do not need to fasten it to the rack.

* Note:

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



Mounting Branch Gateway in the rack

About this task

You can mount the Branch Gateway in a standard 19-inch rack. If the rack has another equipment installed, place Branch Gateway so as to prevent imbalance.

An empty Branch Gateway weighs under 11 lb (5 kg) and between 13 and 14 lb (between 6 and 7 kg) when equipped with the media modules. An empty EM200 weighs under 11 lb (5 kg) and between 12 and 13 lb (between 5 and 6 kg) when equipped with media modules.

Before you begin

- Ensure that the Branch Gateway power supply is disconnected.
- Ensure that the rack is bolted to the floor and is earthquake-protected, if required.
- Attach mounting brackets.

Procedure

1. Place the Branch Gateway in the rack.
Ensure that there is enough space for ventilation.
2. Ensure that the screw holes are aligned with the rack hole positions.
3. Insert four rack mounting screws, two on each side.
4. Ensure that the Branch Gateway is level.
5. Tighten the rack mounting screws.
Do not over-tighten the screws.

Placing Branch Gateway on a table

About this task

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

Procedure

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

Wall mounting requirements

To mount Branch Gateway on a wall, use two wall mounting brackets. You can also use an additional mounting bracket with cable guides.

You must fasten the Branch Gateway to a plywood board. If the wall does not have a portion of plywood available, mount a plywood sheet, at least $\frac{3}{4}$ in. (2.0 cm) thick and 4 x 4 ft (1.2 x 1.2 m) in size, horizontally onto the wall. Use a minimum of four wood screws and ensure the screws are driven into wall studs, or use four wall anchors rated with a shear strength of more than 50 lb (22.5

kg) each. To secure the Branch Gateway to the plywood, use a minimum of four pan head screws of 3/4 inch. Ensure you have the plywood and mounting equipment hardware.

⚠ Caution:

If you install Branch Gateway in the United States of America:

- Do not attach the AC power supply cord to the building wall with wire staples, clamps, and other fasteners.
- You must install Branch Gateway near the AC receptacle (socket outlet) that services Branch Gateway.
- 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 down to the floor, or routed in any way that can lead to its damage.

Mounting the Branch Gateway on a wall

About this task

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

Procedure

1. Attach a wall mounting bracket to each side of the Branch Gateway, as shown in the following image.



2. Mark the plywood with the location of the Branch Gateway bracket screw holes before fastening the plywood to the wall.
3. Place the Branch Gateway with its front panel facing up.
4. Secure the Branch Gateway to the plywood with screws.

Related links

[Brackets with cable guides](#) on page 27

Installing the EM200 expansion modules

About this task

You can extend G430 by attaching one or two EM200 expansion modules. You can mount the EM200 expansion modules in a rack or on a table, similarly to how you mount G430. You cannot mount a G430 with EM200 modules on a wall.

The cables attaching the EM200 expansion modules to G430 are short, so you must install G430 and EM200s one above the other. If you are mounting G430 and EM200 modules on a table, always place G430 on top of the EM200s. In this case, you can open G430 cover if you need to add or replace a DSP module or the RAM card.

Procedure

1. Mount one or two EM200s on a table or in a rack.

G430 mounting procedure applies to mounting EM200s.

2. Connect one end of the expansion cable to the CONNECTOR OUT 1 connector on the rear of G430.
3. Connect the other end of the expansion cable to the CONNECTOR IN connector on the rear of the EM200.



4. If you install two EM200, connect the second EM200 to the CONNECTOR OUT 2 connector on the rear of G430.

Related links

[Branch Gateway chassis mounting](#) on page 26

Media module installation

When the Branch Gateway chassis and optionally the EM200 module(s) are installed, you can install media modules. Each module is shipped with two thumb screws for fastening to the Branch Gateway or EM200 chassis.

Do not install an unsupported combination of media modules. Install media modules only to permitted slots.

* Note:

The required media modules are sometimes pre-installed in the Branch Gateway or EM200 chassis. In this case, skip media modules installation.

Limitations of media module combinations

The Branch Gateway 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, MM710B, MM711, MM712, MM714, MM714B, MM716, MM717, MM720, MM722
- Up to four MM721 modules

*** Note:**

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

Slot allocation

The Branch Gateway chassis has three media module slots, marked V1, V2, and V3. Each of the two optional EM200 expansion modules has two media module slots. The EM200 slots connected to the EXPANSION OUT 1 connector on the rear of the G430 Branch Gateway are slots V5 and V6. The EM200 slots connected to the EXPANSION OUT 2 connector on the rear of the G430 Branch Gateway are slots V7 and V8.

Allocate a slot for the media module. Ensure your media module matches the allocated slot.



1	System (SYSTEM) LEDs	7	10/100M ETH WAN port
2	RST button	8	10/100M ETH LAN ports (10/100/1000 in G430 hardware vintage 3)
3	ASB button	9	Compact Flash (CMPCT FLSH) slot
4	USB 2.0 ports	10	V1: slot for a media module or S8300 Server
5	CCA (Contact Closure) port	11	V2: slot for a media module
6	10/100M Services (SVCS) port	12	V3: slot for a media module

Figure 1: The G430 Branch Gateway front panel ports and slots



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

Figure 2: The EM200 front panel slots

Table 1: Permitted slots for Branch Gateway 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
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

Table continues...

Media module	Permitted slots	Description
MM721	V1-V3, V5-V8	8 ISDN BRI trunk or endpoint (telephone or data) ports
MM722	V1-V3, V5-V8	2 ISDN BRI trunk ports
S8300	V1	Avaya Aura® Server

Media module installation precautions

You can bend or damage the connector pins if you roughly handle the module or misalign it and then force into position.

Electrostatic alert:

Hold the module 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 antistatic bag.

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 equipment damage.

To eliminate electrical hazards for unauthorized personnel and ensure continued compliance to radiated emissions requirements, you must securely tighten all captive screws so that they cannot be loosened without the use of a tool.

After installing media modules, cover empty slots with the supplied blank plates. Using Branch Gateway and EM200 with open slots can cause overheating due to inadequate air distribution.

Installing S8300 Server

About this task

You can install an S8300 Server in slot V1 on the left side of the Branch Gateway.

Procedure

1. Remove the plate above slot V1.
2. Remove the blank plate from slot V1.
3. Align the server with the V1 bay opening and engage both sides of the module with the interior guides.
4. Slide the server slowly into the chassis, maintaining even pressure to ensure that the module does not get twisted or disengaged from the guides.



5. Apply firm pressure to engage the connectors.

The connector has pins of different length. Long pins get engaged first to provide grounding. Medium and short length pins provide power and signal.

6. Tighten the spring-loaded captive screws to lock the media module into the chassis.
 7. Remove the plate labeled **Remove before removing or inserting S8300 module** above the slot V1.
 8. After you insert the server module, insert the other media modules.
- Make sure to insert each module in a slot corresponding to the module type.

Installing media modules

About this task

After you instal an S8300 Server module, if applicable, install media modules. Make sure to insert each module in the corresponding slot.

Procedure

1. Remove the blank plate from the empty bay.
2. Align the media module with the selected bay on the front of the Branch Gateway or EM200 chassis and engage both sides of the module with the interior guides.
3. Slide the module slowly into the chassis, maintaining even pressure to ensure that the module does not get twisted or disengaged from the guides.



4. Apply firm pressure to engage the connectors.
- The media module connector has pins of different length. Long pins get engaged first to provide grounding. Medium and short length pins provide power and signal.
5. Tighten the spring-loaded captive screws to lock the media module into the chassis.

Next steps

After you connect the phones to the various media modules, add circuit protection to the lines.

General grounding requirements

For safe installation and operation of the Branch Gateway, carefully read all requirements, recommendations, and instructions.

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

Grounding requirements differ widely among countries. With addition to the grounding instructions in this section, you must follow the local electrical installation codes for your location.

For AC powered systems, the following two safety grounds are required to ensure safe operation of each Branch Gateway and each EM200:

- The ground conductors in the AC power cords.
- The supplementary ground conductor, a field-installed green and yellow conductor.

Connect all of the safety grounds to an approved ground. If a power cord accompanies the Branch Gateway or EM200, use that cord whenever possible.

 Warning:

Ensure that you follow grounding recommendations. Otherwise, the system:

- Becomes unsafe for personnel handling or using the equipment.
- Is not adequately protected from lightning or power transients.
- Is subjected to service interruptions.

Installation location

When selecting a location for the Branch Gateway or EM200 installation, ensure that you can connect it to the supplied secondary ground conductor. If the location does not meet this requirement, contact a licensed electrician to install a supplementary ground conductor per Article 250 of the National Electrical Code (NEC).

Supplementary ground conductor

A supplementary ground conductor is provided with the equipment. It is constructed of a 10 AWG (4.0 mm²) wire, with an insulated ring terminal crimped to one end, which is suitable for the #8 (M4) stud or screw on the rear of the Branch Gateway or EM200 chassis.

You need to provide a means of connecting the supplementary ground conductor to an approved ground according to Article 250 of the National Electrical Code (NEC).

Ground block

When installing multiple Branch Gateway devices or EM200 modules, use the ground block supplied by the customer. Only a licensed electrician can install the ground block.

The ground block intended for rack mounting has ten terminals for terminating supplementary ground conductors. You can ground up to ten Branch Gateway devices or EM200 modules at the block, installed on a rack close to the equipment. Then you can route a single ground conductor from that block to an approved ground.

 Danger:

Failure to install all safety grounds provided with the Branch Gateway voids the UL and the CE mark product safety certifications. It is hazardous and can cause death or severe personal injury.

Restricted access location (RAL)

In Finland, Norway, and Sweden, G430 and EM200 devices must be installed in a restricted access location, due to unreliable earthing concerns. Only service personnel or customers who have been instructed about the restricted access, and safety precautions can access RAL. Service personnel can access G430 or EM200 devices using a tool, such as a lock and key, or other means of security.

Warning:

For installations in Finland, Norway, and Sweden, the AC powered G430 and EM200 rely on two ground connections: mains plug with an earth contact and a supplementary ground conductor.

Approved grounds

There are two methods for equipment grounding.

- Based on NFPA 70: National Electrical Code (NEC). You must comply with NFPA 70: NEC or with the equivalent local electrical code or grounding requirements.
- Based on ANSI/EIA/TIA-607 Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications (TIA-607), which provides an enhanced, communication-specific grounding scheme.

Important:

Ensure that approved grounds are accessible from the installation site and that a trained technician or licensed electrician all grounds and a supplementary ground conductor.

If required, hire a certified power contractor or auditor prior to system installation or cutover.

NFPA 70: NEC

Compliance with NFPA 70: NEC provides suitable grounding for the Avaya equipment.

In buildings without a ground-cabling infrastructure complying with TIA-607, the Avaya equipment must be grounded by connection to the nearest accessible location on approved building grounds. The following are approved grounds in keeping with the NFPA 70: National Electrical Code of the United States (NEC). For additional information regarding these grounds, view NEC, Article 250.52.

AC service panel

AC ground at the AC service panel serving the Avaya equipment.

Danger:

- Do not perform work inside electrical panels unless you are a qualified electrician.
- Do not try to remove bonding conductors without approval from qualified personnel.

Metal water pipe

The water pipe must meet all the following requirements:

- The entire length of the pipe must be visible, except for short sections passing through walls, ceilings, etc.
- The pipe must be metallic through its length, or made electrically continuous by bonding around insulation joints or insulating pipe.
- The pipe must be routed underground for at least 10 ft (3 m).

Where a metal water pipe is used as an approved ground, the following requirements apply to the host building:

- The building must be industrial, commercial, or institutional, where only qualified persons service the water piping.
- The building does not rely only on the metal water pipe for grounding: a supplemental ground is required. For more information, see NEC Article 250.53.

Metal frame of the building

The qualified personnel must connect the metal frame member (I-beam, pillar) to earth by one of the following methods:

- In direct contact with the earth, or encased in concrete that is in direct contact with the earth, for at least 10 ft (3 m).
- To the reinforcing bars of a concrete-encased electrode. The electrode must be 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, 0.5 in. (1.3 cm) in diameter, or at least 20 ft (6.1 m) of bare solid copper, 4 AWG (26 mm²) wire.
- To a ground ring. A ground ring is a buried ground that encircles a building, having a length of at least 20 ft (6.1 m) of 2 AWG (35 mm²) bare copper wire.
- To rod and pipe electrodes. A rod or pipe electrode consists of one 5/8 in. (1.6 cm) solid rod or 3/5 in. (2 cm) conduit driven to a minimum depth of 8 ft (2.4 m).
- To plate electrodes. Plate electrodes have a minimum of 2 ft² (0.185 m²) of metallic surface exposed to the exterior soil.

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 equipment single-point ground terminal. Approved floor grounds can include the following:

- Metal frame of the building.
- The grounding conductor for the secondary side of the power transformer feeding the floor.
- A grounding point specifically provided in the building for that purpose.

Warning:

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

ANSI/EIA/TIA-607

TIA-607 defines an intra-building ground-wiring scheme for communications equipment and specifies equipment connection or grounding points. According to TIA-607, the underlying building grounding infrastructure must be set in compliance with NFPA 70: NEC or the equivalent local electrical code or grounding requirements.

In buildings where a ground-cabling infrastructure complying with TIA-607 has been implemented, the Avaya equipment must be grounded according to the TIA-607 standard. In a TIA-607 installation, the Telecommunications Main Grounding Busbar (TMGB) or Telecommunications Grounding Busbar (TGB) links the telecommunications equipment to the ground.

Other grounding terminology is:

- Building principle ground, normally in a building with one floor.
- Floor ground bar, normally in buildings with more than one floor.

Configure telecommunications subsystems, such as groups of frames or equipment, as separate single-point ground entities connected to the dedicated service panel through a single-point ground bar. The service panel ground connects to the building principle ground through the main service panel or, in a TIA-607 installation, through the TGB.

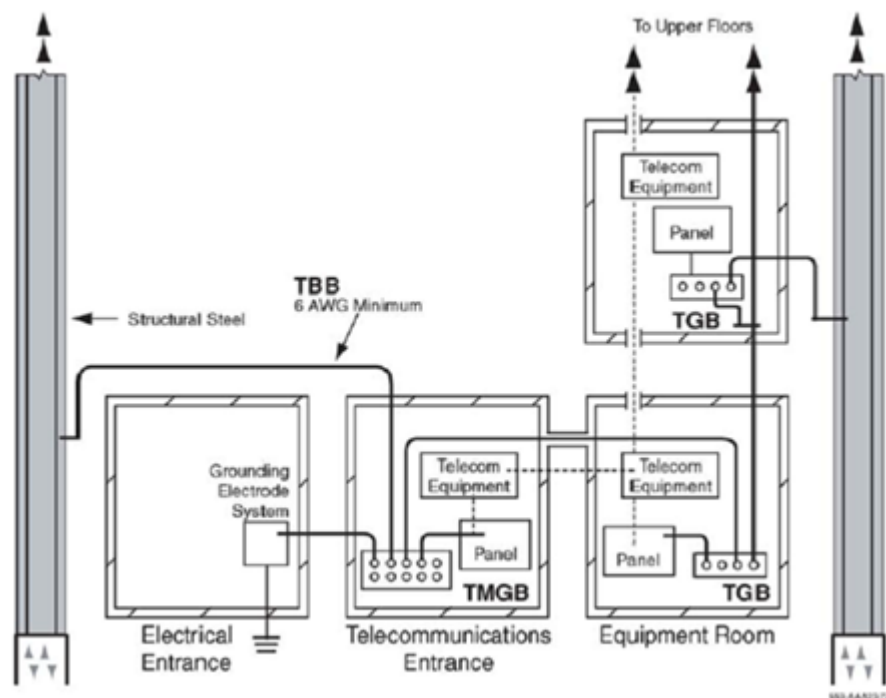


Figure 3: ANSI/TIA/EIA-607 grounding schematic

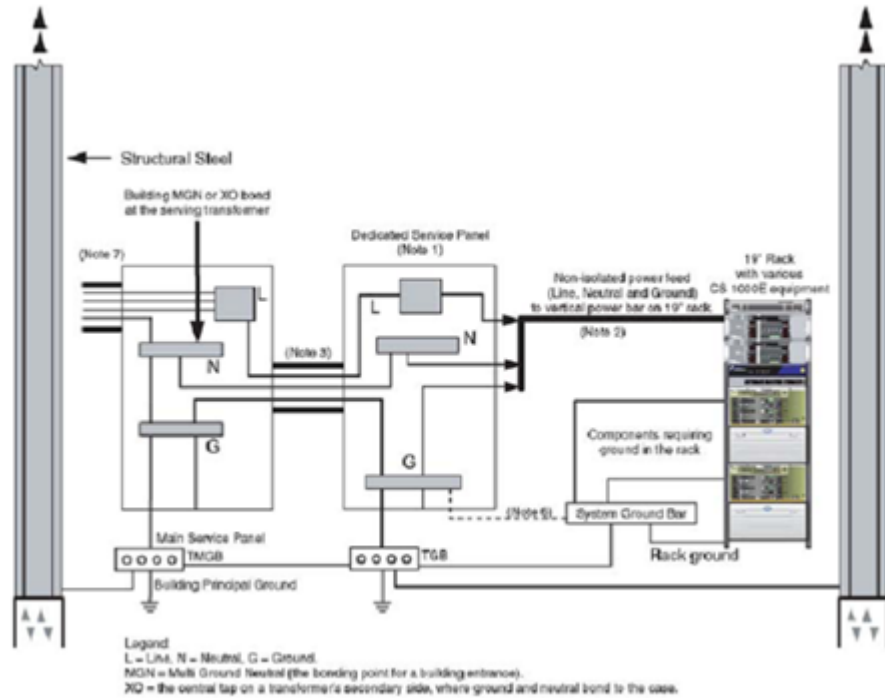


Figure 4: Typical wiring plan

Safety ground connections

Proper grounding of the Branch Gateway and EM200s installation protects the system, users, and service personnel from lightning, power surges, AC mains faults, power crosses on central office trunks, and electrostatic discharge (ESD).

When installing the Branch Gateway or EM200, you must follow the local electrical installation codes.

Danger:

In AC powered systems, connect through both the AC Power Cord and the supplementary ground conductor for safe operation of the Branch Gateway.

Warning:

An improper ground can cause an electrical shock, equipment failures, and service outages.

Attaching the ground wires

About this task

Perform the following procedure for each Branch Gateway and EM200s.

Procedure

1. Unscrew the lock nut of the ground screw on the rear of the chassis adjacent to the ground symbol.
2. Attach the ring terminal end of the 10 AWG (4.0 mm²) supplementary ground conductor on the ground screw.
3. Tightly close the lock nut.

Attaching ground wires to purchased ground blocks

About this task

You can use a ground block with more than one Branch Gateway or EM200 in the rack. If you want to use a ground block, you must purchase it and have it installed by a licensed electrician.

Supplementary ground conductor has one end attached to the grounding screw on the chassis.

Warning:

Do not coil the supplementary ground conductor or ground wire.

Procedure

1. Cut the supplementary ground conductor to the length needed to terminate it into one of the terminals of the ground block.
2. Attach one end of the remaining 10 AWG (4 mm²) ground wire to one of the terminals in the ground block and the other end to an approved ground.
3. Cut the ground wire to the length needed to reach the approved ground.

Attaching ground wires without ground blocks

Procedure

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 Branch Gateway chassis.

Related links

[Connecting Branch Gateway to a power source](#) on page 41

Connecting the EM200 expansion module to a power source

About this task

Before you connect power to G430, you must connect the EM200 expansion modules to a power source.

 Warning:

If you need to move the EM200 expansion modules in a working system consisting of G430 and one or two EM200s housing media modules, you must disconnect the EM200 from a power source before reconnecting the expansion cable to another slot.

Perform the following procedure for each EM200 connected to G430.

Procedure

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

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 G430. This indicates that the two media module slots are considered slot 5 and slot 6 of 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 G430. This indicates that the two media module slots are considered slot 7 and slot 8 of G430.

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

Connecting Branch Gateway to a power source

About this task

You can connect a Branch Gateway to a power source after you have mounted the Branch Gateway, optionally mounted and connected EM200 devices, media modules, and attached the supplementary ground conductor.

Procedure

1. Connect the power cable to the power connector on the Branch Gateway back panel.
2. Plug the AC power cable into an AC wall outlet.

When the Branch Gateway is switched ON, the PWR LED on the front panel comes ON. The CPU LED comes ON if the firmware is running.

At least one LED on each media module, except S8300 Server, comes ON and then goes OFF after about 20 seconds.

Chapter 4: Connecting peripheral devices

You can connect external endpoint devices to the front panel ports of the installed media modules and to the fixed front panel ports. Mount the Branch Gateway, and EM200s if required, and insert all media modules before you connect the endpoint devices.

You must connect peripheral devices in the following order:

1. Data and voice devices
2. Circuit protection
3. Wide Area Network (WAN)
4. Coupled Bonding Conductor (CBC)
5. Avaya Partner Contact Closure Adjunct



Warning:

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

Data and voice device connections

You can connect data and voice devices in various ways. To connect devices to specific ports, refer to your planning documentation for topology requirements. 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 Branch Gateway.

Switch and network data ports

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

IP phone connections

You must connect an IP phone to the external Ethernet switch that has connectivity with G430 Branch Gateway. You can power an IP phone either by the switch or by its own power supply.

For a full list of supported phones, see *Avaya G430 Branch Gateway Overview and Specification*.

Connecting a phone to Branch Gateway

Procedure

1. Connect the phone to a port on the switch connected to the Branch Gateway LAN port.
If the switch is PoE, you do not need to plug the phone into the power supply.
2. Plug the phone into the telephone port.
3. **(Optional)** If the phone is powered independently, do the following:
 - a. Plug the phone into the power supply.
 - b. Check that the phone is powered up.

ISDN BRI station connections

Each ISDN port on the MM720 and MM721 media module supports up to two ISDN BRI stations.

You cannot administer MM720 and MM721 BRI media modules to support both BRI trunks and BRI stations at the same time. However, MM720 and MM721 BRI media modules support combining both B-channels to form a 128-kbps channel. Communication Manager 3.1 supports combining B-channels using BONDing to form a high-bandwidth connection.

If you administer the MM720 or MM721 BRI media module to support BRI stations, you cannot use it as a clock synchronization source.

Connecting an ISDN BRI station to an ISDN port

Procedure

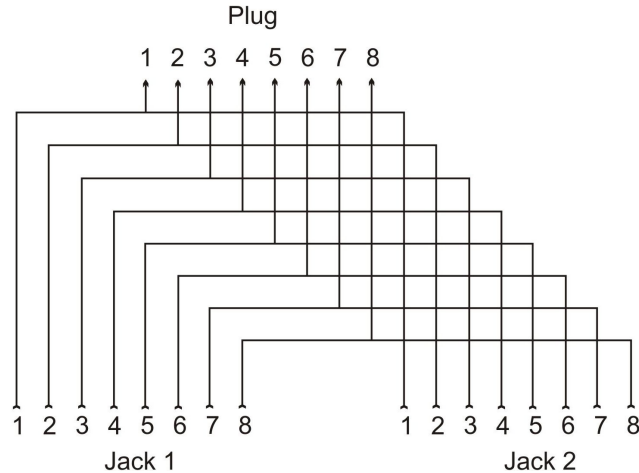
Connect the station via a standard 8-pin BRI cable to one of the ISDN ports on the MM720 media module.

Connecting two ISDN BRI stations to an ISDN port

Procedure

1. Connect each BRI station to an RJ-45 splitter that provides two RJ-45 4-pair jacks and one RJ-45 male connector.

The following image shows the correct wiring for the RJ-45 splitter.



2. Connect the splitter male connector to one of the ISDN ports on an MM720 or MM721 media module.

The following images show the ISDN port location for MM720 and MM721 media modules.

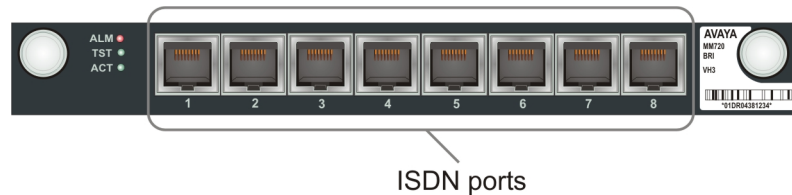


Figure 5: MM720 media module ISDN ports

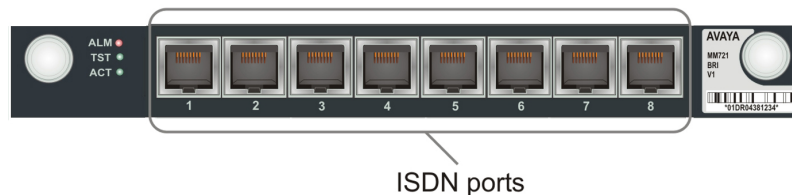


Figure 6: MM721 media module ISDN ports

Connecting an analog phone

About this task

Analog line ports support up to 2,000 ft (609.6 m) for the phone equipment with a ringer load below 3 REN.

For a full list of supported phones, see *Avaya G430 Branch Gateway Overview and Specification*.

Procedure

1. Connect the phone to one of the following analog ports:
 - A universal analog port on an MM711 media module.

- An analog line port on the punch down block connected to an MM716 media module.

To connect the MM716 media module to a punch down block, see [Connecting devices to the MM717 and MM716 media modules](#) on page 48.

- A LINE port on an MM714 or MM714B media module.

2. Plug the phone into the telephone port.

The following images show the analog port location on MM711, MM714, MM714B, and MM716 media modules.

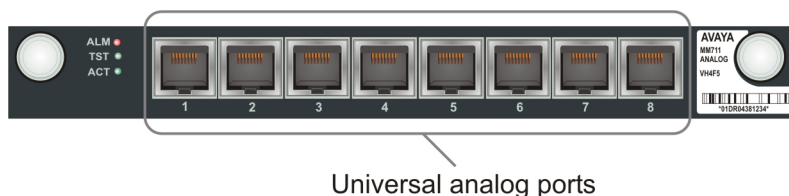


Figure 7: MM711 media module analog ports

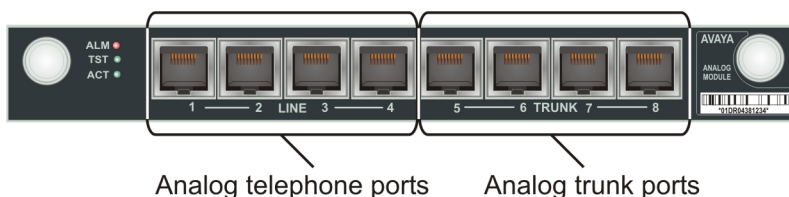


Figure 8: MM714 media module analog ports

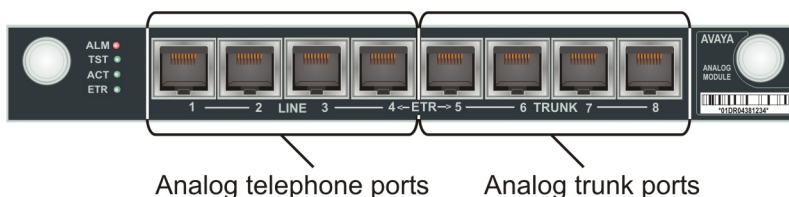


Figure 9: MM714B media module analog ports

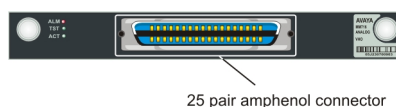


Figure 10: MM716 media module amphenol connector

Connecting a DCP phone to an MM712 or MM717 media module

About this task

The MM712 media module supports 8 DCP ports and the MM717 media module supports 24 DCP ports, via a single 25-pair amphenol socket on the Branch Gateway front panel.

For a list of supported DCP phones, see *Avaya G430 Branch Gateway Overview and Specification*.

Warning:

Avaya MM712 and MM717 DCP lines require 146E IROB protectors, or 4C3S-75 solid-state 5-pin protectors when they are used for any connection routed out-of-building. These protection devices provide both overvoltage and overcurrent protection.

Procedure

Wire a telephone port to a DCP port on Branch Gateway.

The following images show the DCP port location on MM712 and MM717 media modules.

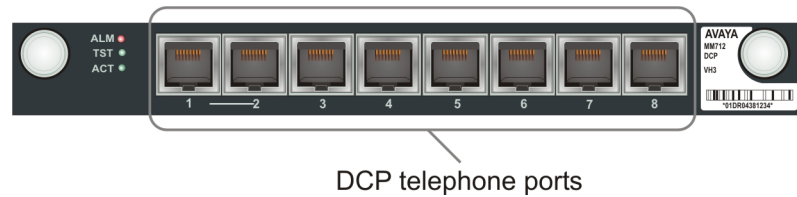


Figure 11: MM712 media module DCP ports

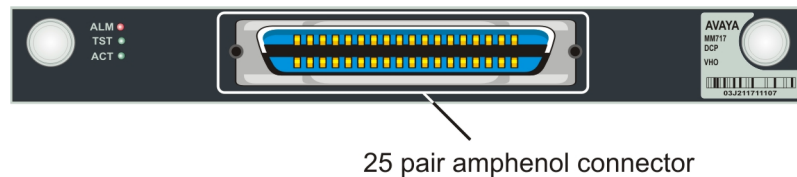


Figure 12: MM717 media module DCP ports

Related links

[Connecting phones to MM716 and MM717 media modules](#) on page 48

Connecting an analog trunk

Procedure

Connect the analog trunk to one of the following ports:

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

Connecting an analog DID trunk

About this task

You can connect a DID trunk to Branch Gateway using one of the compatible ports.

The trunk analog telephone port on the Branch Gateway front panel forms a mechanical analog relay with the LINE port next to it. You can configure this relay to provide emergency transferred telephone service in the case of a power outage or disconnection from an external server. During an emergency situation, all incoming calls on the trunk are directed to the phone plugged into the LINE port. The phone also uses the trunk for outgoing calls.

Procedure

Connect the analog DID 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.
- One of the line ports on an MM714 or MM714B media module.
- The trunk port on the Branch Gateway front panel.

Related links

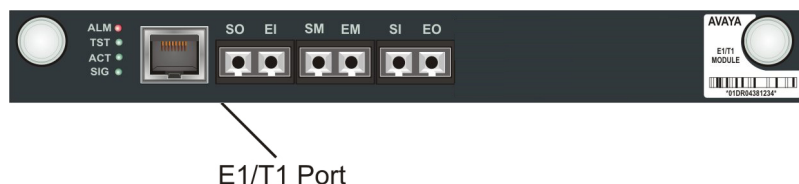
[Connecting phones to MM716 and MM717 media modules](#) on page 48

Connecting an E1/T1 trunk

Procedure

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

The following image shows the E1/T1 port location on an MM710B media module.



The SIG LED lights.

Connecting an ISDN BRI trunk

About this task

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

Procedure

Connect the trunk to any ISDN port on an MM720, MM721, or MM722 media module.

The following images show the ISDN port location on MM720, MM721, and MM722 media modules.

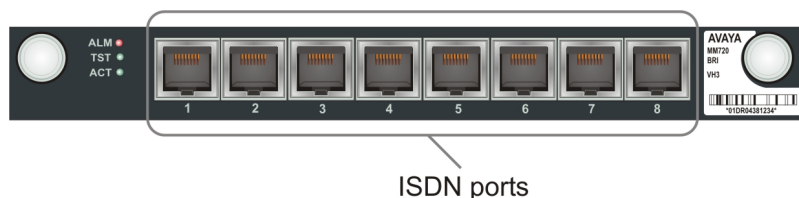


Figure 13: MM720 media module ISDN ports

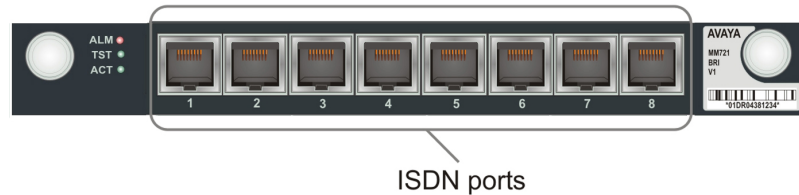


Figure 14: MM721 media module ISDN ports

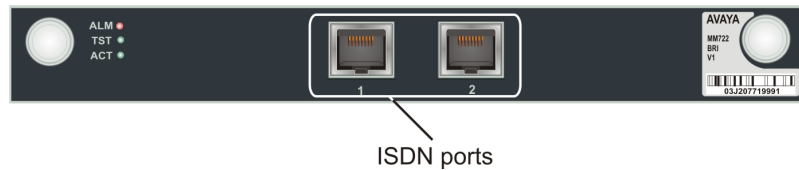


Figure 15: MM722 media module ISDN ports

Connecting phones to MM716 and MM717 media modules

About this task

The MM716 and MM717 media modules have a single 25-pair amphenol socket on the front panel, which you can use with a punch-down block.

Procedure

Connect the front panel connector to a punch-down block.

You can terminate up to 24 phones on the connected punch-down block.

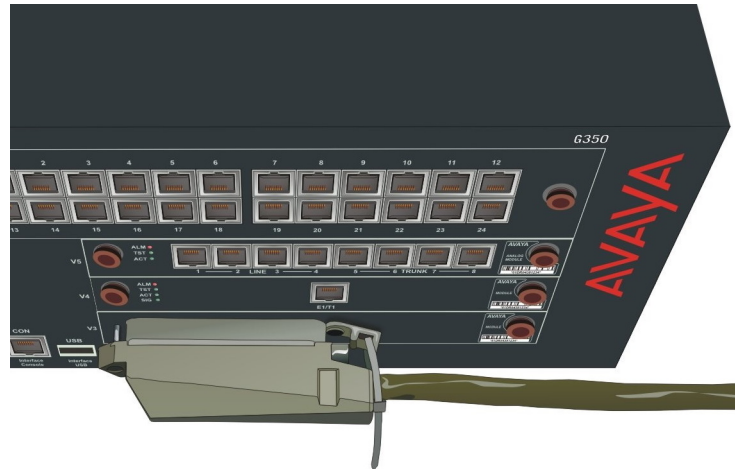
Connecting an MM716 and MM717 front panel connector to a punch-down block

Procedure

1. Connect one end of a CAT-5 cable with a 25-pair amphenol connector at each end to the 25-pair socket on the front panel of an MM716 or MM717 media module.

The cable must allow plugging the connector into the media module at an angle of 90° to the cable.
2. Extend the cable to the right of Branch Gateway.
3. Tighten the end screw of the amphenol connector to securely fasten the connector to the left side of the front panel socket.
4. Thread a tie wrap through the small bracket to the right of the front panel socket.
5. Fasten the tie wrap around the cable to secure the cable to the right side of the front panel socket.

The following image shows attaching and securing an amphenol cable to the MM716 or MM717 25-pair socket.



6. Connect the other end of the amphenol cable to a punch-down block that converts the single amphenol connector to 24 RJ-11 jacks.

You can now connect endpoint devices to the RJ-11 jacks.

Related links

[MM716 ports](#) on page 122

[MM717 ports](#) on page 123

Circuit protection installation

All out-of-building trunks, lines, and terminal installations require protection from sneak currents and over-voltages, such as lightning and power line induction. Campus installations (interbuilding cabling) of phones or other standard devices require over-voltage and sneak current protection in both buildings. You must install over-voltage and sneak current protectors in accordance with subsections “Protective Devices” and “Cable and Primary Protector Bonding and Grounding” of NFPA 70: NEC Article 800 , or local safety codes.

Field installed sneak current protectors must have a maximum current rating of 350mA and a minimum voltage rating of 600V.

The following over-voltage and sneak current protection devices are approved for use with G430 Branch Gateway:

Media modules	Approved over-voltage and sneak current protection devices
Avaya MM710 and MM710B media modules	Over-voltage and sneak current protection for these interfaces are provided on the media modules themselves.

Table continues...

Media modules	Approved over-voltage and sneak current protection devices
Avaya MM711, MM714, MM714B, and MM716 analog media modules	Over-voltage and sneak current protection for these interfaces is provided on the media modules themselves. Normally, the local phone company provides primary over-voltage protection for incoming trunks. Analog voice terminals require 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 (In-Range Out-of-Building). 146C (4 - lines) or 146H (25 - lines)
Avaya MM712 and MM717 DCP media modules	Out-of-building connections require either the 146E IROB or 4C3S-75 solid state protectors for over-voltage and sneak current.
Avaya MM722 ISDN-BRI media modules	Over-voltage and sneak current protection are provided on the media modules themselves.
Avaya MM720 and MM721 ISDN-BRI media modules	All out-of-building installations on both trunk (network) and line (customer) sides require either the 146E IROB or 4C3S-75 solid state protectors for over-voltage and sneak current. Trunk side applications also require an NT-1 device.

**Warning:**

Only service-trained personnel can install these circuit protection devices.

Coupled Bonding Conductor installations

The Coupled Bonding Conductor (CBC) provides mutual inductance coupling between the CBC and the phone cables that are exposed to lightning. The conductor can be a 10 AWG (4 mm²) wire tie wrapped to the exposed cables, a metal cable shield around the exposed cables, or six spare pairs from the exposed cable. In a high-rise building, connect the CBC to an approved building ground on each floor.

Installing the CBC

Before you begin

Ensure the phone lines are cross-connected to the required media module.

Procedure

1. Connect one end of the conductor to a phone cable building entrance protector ground that is connected to an approved ground.

2. Route the rest of the conductor next to the exposed phone cables being protected until they reach the cross-connect nearest to the phone system.
3. Connect the other end to the single-point ground block provided for the phone system.

You must place the non-exposed phone cables at least 12 in. (30.5 cm) away from the exposed phone cables.

Avaya Partner Contact Closure Adjunct installations

The Contact Closure feature is a controllable relay providing dry contacts for various applications. To implement the contact closure feature, you must connect an Avaya Partner Contact Closure Adjunct box to the CCA port on the Branch Gateway chassis. The adjunct box provides two contact closures that you can operate in 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. You can configure the CCA port so that an end device, such as a phone, can control the connected devices. For example, a user can unlock a door by keying a sequence into a phone keypad.

Installing the contact closure

About this task

To connect the Avaya Partner Contact Closure adjunct box to the Branch Gateway, use a 24 gauge minimum phone wire, no longer than 200 ft, with a standard four wire RJ-11 connector.

During the installation, note which device you connect to each relay. You will need this information for configuration.

Procedure

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, which the Contact Closure relays activate and deactivate.
2. Connect the Avaya Partner Contact Closure adjunct box to the CC port on the Branch Gateway front panel.

Chapter 5: Connecting and enabling a USB modem for remote access

Modems for remote access

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

If S8300 is installed in Branch Gateway, leave a modem connected permanently to enable reporting of alarms to remote locations.

Modem access is not supported if FIPS mode is enabled in the gateway.

Chapter 6: Branch Gateway configuration

The Branch Gateway requires software configuration. The Branch Gateway can be configured by using the Avaya Branch Gateway Command Line Interface (CLI). The CLI is a comprehensive tool for configuring the gateway and includes all supported configuration tasks. For information about configuration by using the CLI, see *Administering Avaya G430 Branch Gateway*. For information about CLI commands, see *Avaya Branch Gateway G430 CLI Reference*.

The Branch Gateway can be accessed:

- At the customer site through a laptop connected to the Services (SVCS) port of the Branch Gateway.
- Remotely through the network. For information about preparing a newly installed Branch Gateway for configuration through the network, see [Configuring basic Branch Gateway connectivity](#) on page 53.
- From a remote location through a modem.

Configuring basic Branch Gateway connectivity

About this task

You can run an installation script on a newly installed Branch 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.

Procedure

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 to the Branch Gateway Services (SVCS) port using an Ethernet cable.
4. SSH to 192.11.13.6.

5. At the prompt, enter the default username: `root` and password: `root`

6. At the prompt, configure a new password.

Follow the password complexity rules while setting a new password. For password rules, see *Avaya Branch Gateway G430 CLI Reference*

7. At the **Enhanced Access Security Gateway (EASG)** prompt, read the following message:

```
*****
```

```
Enhanced Access Security Gateway (EASG) Confirmation.
```

```
*****
```

```
Please confirm whether Avaya is granted login access this system.  
You may change this setting any time after confirmation is  
completed.
```

```
Enable EASG: (Recommended)
```

```
By enabling Avaya Logins you are granting Avaya access to your  
system.
```

```
This is necessary to maximize the performance and value of you  
Avaya
```

```
support entitlements, allowing Avaya to resolve product issues in a  
timely manner.
```

```
In addition to enabling the Avaya Logins, this product should be  
registered with Avaya and technically onboarded for remote  
connectivity
```

```
and alarming. Please see the Avaya support site  
(support.avaya.com/registration) for additional information for  
registering products and establishing remote access and alarming.
```

```
Disable EASG:
```

```
By disabling Avaya Logins you are preventing Avaya access to your  
system.
```

```
This is not recommended, as it impacts Avaya's ability to provide  
support
```

```
for the product. Unless the customer is well versed in managing the  
product themselves, Avaya Logins should not be disabled.
```

```
Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG? 1
```

8. At the prompt, enter 1 or 2 to enable or disable EASG.

The following message is displayed:

```
Do you want to continue (Y/N)?
```

9. At the prompt, enter `Y` to continue.

10. At the prompt, enter `Y` to configure basic gateway connectivity.

If you enter `n`, you can use the **script-config** CLI command to run the installation script, as long as you have not saved any configuration changes you may have made.

If you need to configure the gateway in FIPS mode, enter `n` and run the command **set fips-mode enable**. The command will remove the existing configuration and resets the gateway. After the reset, repeat from step 4 above.

11. Configure the following parameters:

For each parameter, you can enter a value, or click **Enter** to accept the default value shown in square brackets:

- VLAN number
- IPv4 enabled or disabled
- Static IPv4 address
- IPv4 address for the primary management interface
- IPv4 Subnet mask for the primary management interface
- IPv4 address for the default gateway (router)
- IPv6 enabled or disabled
- IPv6 Unicast global address.
- IPv6 prefix length
- IPv6 Link local address
- IPv6 PMI (Global or Link Local)
- IPv6 Default gateway
- Up to eight IP addresses (four IPv4 and four IPv6) to specify the Media Gateway Controllers
- Hostname for the Branch Gateway

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

- If you confirm the settings, they are saved and the Branch Gateway 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.

12. Connect the Ethernet port to the network to enable remote access to the Branch Gateway.

A remote technician can now further configure the Branch Gateway using the CLI.

Chapter 7: Post-installation verification

After the initial configuration, you must verify if the installation has been successful and remove the installation equipment.

Roadmap for post installation

Perform these post-installation procedures in the following order using the appropriate procedure described in this section:

1. Test the installation
2. Remove the installation equipment

Installation testing

When the installation is complete, you must perform simple tests to verify telephone and data connectivity.

Testing data connectivity

About this task

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

Procedure

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

About this task

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 Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Testing LSP failover

About this task

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

* Note:

If SLS mode is enabled and the primary controller and LSP fail, then the Branch Gateway enters SLS mode.

For more information about testing LSP failover, see “Auto Fallback for H.248 Gateways” in *Administering Network Connectivity on Avaya Aura® Communication Manager* and the Migrate H.248 MG to primary” screen command in *Avaya Aura® Communication Manager Screen Reference*.

Procedure

1. Verify that valid translation 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 addresses for the primary controllers) (MGC). If you are using Avaya IW to configure Branch Gateway, the following are the key actions that must be done in the wizard to ensure correct IP address configuration:

- a. On the Usage options screen, install an LSP that is associated with an S8300 server Primary Controller.

After you select the usage option, the Primary Controller IP Address screen appears and calls for the required addresses for your primary controller type. Configure the following IP address for each primary controller type:

Primary media gateway controller	Number of IP addresses to be configured	IP addresses to configure
S8300 server	1	The IP address of the primary S8300 server

- b. On the Primary Controller IP Address screen, enter all the required IP addresses for the primary controller type.

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

You must add the LSP server correctly to the Main Communication Manager server.

2. If valid translations are not file synchronized to the LSP, do the following:
 - a. From a SAT session running on 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 Branch Gateway from the primary controller, ensuring that all telephones are still connected or have network connectivity to the Branch Gateway.
4. Verify that you can make calls between local telephones using the outside lines connected locally to the Branch Gateway.

IP addresses and controllers

The IP address of the Communication Manager's CLAN or the IP address of an Ethernet Port on the server on which Communication Manager is deployed which is used for processor Ethernet Connections.

Removing the installation equipment

About this task

Remove all equipment that you used during the installation process. This may include the CD-ROM drive, the software upgrade CDs, the laptop computer, and the modem (for installations without an S8300 server module only).

Chapter 8: Media module and device additions

When adding new devices to the Branch Gateway, consult your project manager for topology requirements for connections between specific ports and specific devices.

Media module additions

Various media modules can be added to the Branch Gateway.

Voice module additions

You can hot-swap voice modules. This means that you can add or remove a voice module in the Branch Gateway or EM200 while the system is running, without any disruption to your network. Configuration of the Branch Gateway 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 59 and [Adding a trunk](#) on page 61.

Some configuration of the Avaya Aura® Communication Manager is necessary when you install an MM710, MM710B, MM720, MM721, or MM722 media module. See *Administering Avaya Aura® Communication Manager*. Also, for an MM710, MM720, MM721, or MM722, it is usually advisable to set the media module as the synchronization source of the Branch Gateway. For information about setting the synchronization source of the Branch Gateway, see the *Avaya Branch Gateway G430 CLI Reference*.

Telephone additions

You must connect, configure and test the telephone before adding the telephone to the Branch Gateway.

Telephone connections

To connect a new telephone, see the following sections:

- [Connecting an IP telephone](#) on page 42
- [Connecting an analog telephone](#) on page 44
- [Connecting a DCP telephone to an MM312, MM712, or MM717 media module](#) on page 45

Configuration of telephones on Communication Manager

Standalone:

- Media gateway phones are configured on Avaya Aura® Communication Manager, see the *Administering Avaya Aura® Communication Manager* guide for more information.
- LSP: Configuration is done on the primary Communication Manager server.

For information about connecting a laptop to the Services (SVCS) port, see [Connecting a computer to the Services \(SVCS\) port](#). For information about preparing a modem, see Chapter 4: Connecting and enabling a modem for remote access. For information about configuration, see [Branch Gateway configuration](#) on page 53.

Telephone information recordings 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 Branch Gateway to which the telephone connects — this does not apply to IP telephones.

Testing the telephone

Procedure

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.

Trunk additions

You must order, connect, configure, and test the trunk before adding the trunk to the Branch Gateway.

Trunk ordering

- Make sure that the telephone service provider installs the trunk near the physical location of the Branch Gateway 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. 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

Trunk configurations on Communication Manager

- Trunks on the media gateway are configured on Avaya Aura® Communication Manager, see the Communication Manager administration guide for more information.
- LSP: Configuration is done on the primary Communication Manager server.

 Note:

Sync timing configuration for a T1/E1 trunk is done through the CLI or the Communication Manager administration interface.

For information about connecting a laptop to the Services (SVCS) port, see [Connecting a computer to the Services port](#). For information about preparing a modem, see [Chapter 4: Connecting and enabling a modem for remote access](#). For information about configuration, see [Branch Gateway configuration](#) on page 53.

Trunk information recordings for software configuration

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

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

Testing the trunk

Procedure

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 Branch Gateway trunk.

Broadband line additions

You must order, connect, configure and test the Broadband line (xDSL or cable modem) before adding the line to the Branch Gateway.

Broadband line ordering

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

Broadband line connections

Connect a Broadband line.

Broadband line configuration

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

For information about connecting a laptop to the Services (SVCS) port, see [Connecting a computer to the Services \(SVCS\) port](#). For information about preparing a modem, see [Chapter 5: Connecting and enabling a USB modem for remote access](#) on page 52. For information about configuration, see [Chapter 6: Branch Gateway configuration](#) on page 53.

Testing the Broadband link

About this task

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

Avaya Partner Contact Closure Adjunct additions

To install an Avaya Partner Contact Closure Adjunct, follow the instructions in [Installing the Avaya Partner Contact Closure Adjunct](#) on page 51.

Chapter 9: Field Replaceable Unit upgrades and replacements

You can add or remove VoIP modules, the fan tray, or a power supply unit. You can add or replace a VoIP module, as well as add or remove components of the upgrade memory kit. Refer to Equipment list for ordering information.

Note:

The G430 v1 has an on board MP20. However, if an MP120 is installed on G430 v1, the on board MP20 will be disabled. G430 v2 has no on board media processor but a pre-installed MP120 module. You can identify the G430 version by determining either the C/S number on the label or the comcode number.

Inserting or removing an MP10, MP20, MP80, or MP120 VoIP module

About this task

G430 v1 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, MP80, or MP120 VoIP module. If an MP120 is installed on G430 v1, the on-board VoIP module is disabled. G430 v2 has no on-board VoIP module.

The G430 hardware vintage 3 (G430 v3) has one on-board VoIP module providing 40 channels of G.711, G.726, G.729, with feature set including V.150.1 as the MP120. The G430 v3 only accepts the MP120 VoIP module. If MP120 is installed on the G430 v3, the on-board VoIP module is disabled.

Note:

The MP120 is capable of supporting new media services such as V.150.1. In the past, all DSP cards were capable of supporting all codec types with various performance differences in terms of point costs. However, the V.150.1 protocol is not supported on the older DAR cards.

G430 supports a maximum of 120 channels. If MP120 is installed on a G430 v1, the on-board VoIP module will be disabled.

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.

Procedure

1. To remove the G430 cover, see [Removing the G430 cover](#) on page 65.
2. To insert a VoIP module, see [Inserting a VoIP module](#) on page 66.
3. To remove a VoIP module, see [Removing a VoIP module](#) on page 68.

Skip this step if you are inserting a module into an empty slot.

4. To install the G430 cover, see [Replacing the G430 cover](#) on page 69.

Removing the G430 cover

About this task

Voltage:

Disconnect the G430 gateway from the external power source before proceeding.

Electrostatic alert:

Do not touch any components on the printed circuit board.

Procedure

1. Disconnect the power cable from the mains power supply.
2. Make a note of the cable connections, so that you can reconnect them correctly.
3. Disconnect all cables (data and power) connected to the G430 gateway and the media modules, both front and rear.
4. Remove the G430 gateway from the rack or wall.
5. If applicable remove the mounting brackets are attached to the G430.
6. Remove the 8 cover screws, indicated by small arrows etched into the cover:
 - Remove one screw from the top (see [the figure](#) on page 65).
 - Remove four screws from the right side (see [the figure](#) on page 66).
 - Remove three screws from the left side (see [the figure](#) on page 66).
7. Lift the cover off the G430 gateway.



Figure 16: Removing the G430 cover screw from the top of the device

*** Note:**

POE POWER INPUT connector is not present in G430 (v2 or v3).

Table 2: Figure notes:

- a. G430 top cover screw



Figure 17: Removing G430 cover screws from the right side

Table 3: Figure notes:

- a. G430 right-side cover screw
- b. G430 right-side cover screw
- c. G430 right-side cover screw
- d. G430 right-side cover screw



Figure 18: Removing G430 cover screws from the left side

Table 4: Figure notes:

- a. G430 left-side cover screw
- b. G430 left-side cover screw
- c. G430 left-side cover screw

Inserting a VoIP module

About this task

⚠ 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.

Procedure

1. The lower board for the MP120 has a plastic standoff. Insert the plastic standoff to MP120.

*** Note:**

This step is applicable only for MP120 installation.

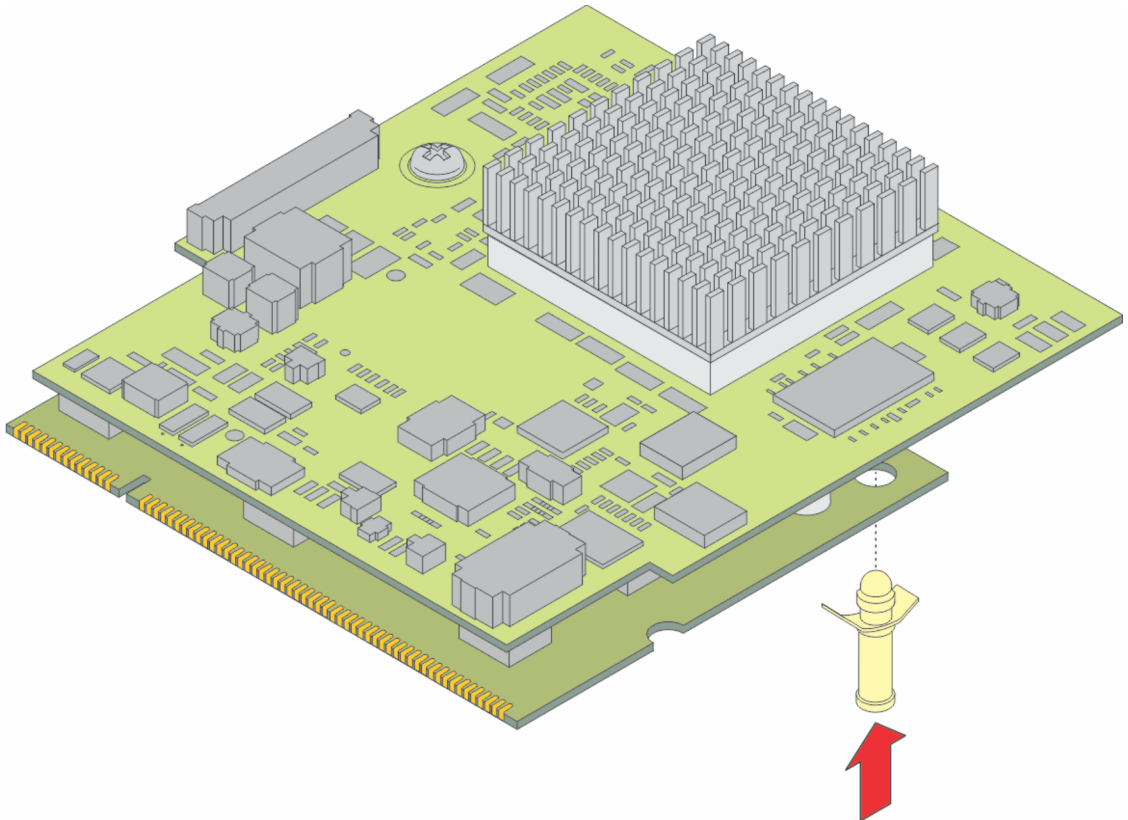


Figure 19: Insert plastic standoff

2. Locate the VoIP module slot (see [the figure](#) on page 68).
3. Position the VoIP module at a 45 degree angle to the main board, and start inserting it into the VoIP module slot (see [the figure](#) on page 68).

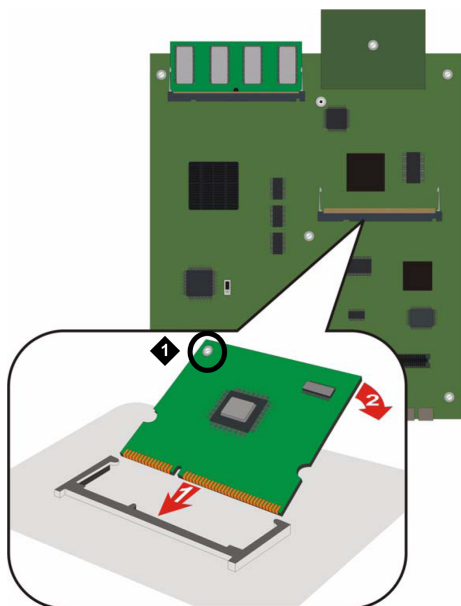


Figure 20: Inserting a VoIP module into the VoIP module slot

Table 5: Figure notes:

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

Removing a VoIP module

About this task

Electrostatic alert:

Hold the module 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 antistatic bag.

Caution:

The connector pins can be bent or damaged if the module is handled roughly or if you misalign the module before forcing the module into position.

Procedure

1. Locate the VoIP module slot (see [the figure](#) on page 66).

2. Unscrew the locking screw attaching the VoIP module to the motherboard (see [the figure](#) on page 66).
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

About this task



Electrostatic alert:

Do not touch any components on the printed circuit board.

Procedure

1. Put the cover back on the G430 gateway unit.
2. Install the 8 cover screws.
Their locations are indicated by small arrows etched into the cover:
 - One screw on the top (see [the figure](#) on page 65).
 - Four screws on the right side (see [the figure](#) on page 65).
 - Three screws on the left side (see [the figure](#) on page 65).
3. If applicable install the mounting brackets to the G430 gateway.
4. Put the G430 gateway in the rack or mount on the wall.
5. Re-connect all cables (data and power) that you disconnected from the G430 gateway and its media modules, both front and rear.
6. Connect the power cable to mains socket.
7. Use the **show platform mainboard** CLI command to make sure the G430 gateway is working properly.

For example, when the G430 gateway is working properly, output includes:

```
MAINBOARD BOARD
-----
Type                : G430
Description         : Avaya Inc., G430 Media Gateway
Serial Number       : 08IS26191007
HW Vintage          : 3
HW Suffix           : A
FW Version          : 42.4.0
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                : MP120 VoIP DSP Module
Description         : VoIP DSP resource with 120 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
```

Installation of the upgrade memory kit

By using the upgrade memory kit, you can increase the number of announcement files on the G430 from 256 to 1024 by storing the files on a removable compact flash. You can also increase the total announcement time from 45 minutes to 4 hours. However, because the announcements are played from RAM, you must also increase RAM to 512 MB.

Note:

The G430 hardware vintage 3 does not require a new memory card. For more information about checking the hardware vintage, see [Checking the G430 hardware vintage](#) on page 83.

The upgrade memory kit contains:

- One 1 GB compact flash memory card
- One memory card with 512 MB of RAM: Only for G430 v1 and G430 v2

The upgrade memory kit

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](#) on page 65.
2. [Replacing The RAM card](#) on page 71.
3. [Replacing The G430 cover](#) on page 69.

RAM card replacement

About this task

Electrostatic alert:

Hold the module 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 antistatic bag.

Procedure

1. Locate the RAM slot (see [the figure](#) on page 72).
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.

Result

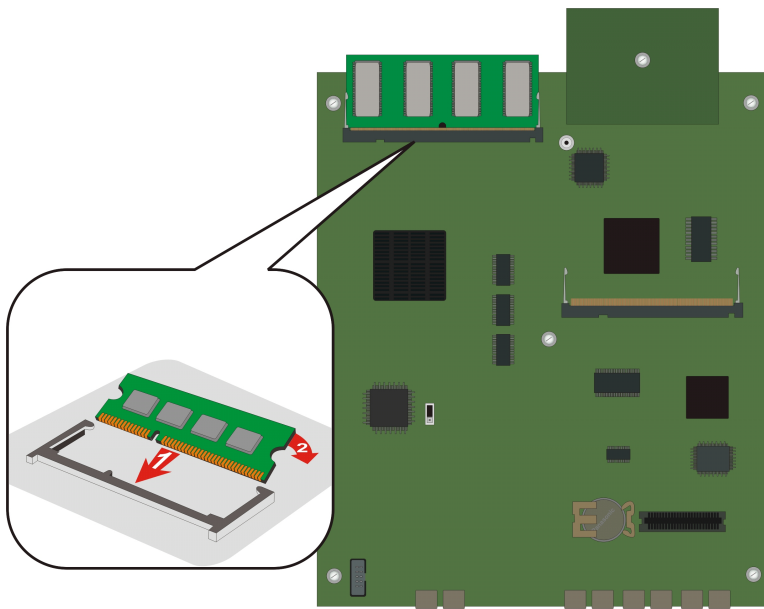


Figure 21: Replacing the RAM card

* Note:

RAM card replacement is applicable only for G430 v1 and G430 v2.

Compact flash memory cards

The Branch Gateway 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

Procedure

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 (CMPCT FLSH) memory card so that the vendor name faces up and the connector points toward the Branch Gateway, and gently insert it into the compact flash slot.

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.

3. To move the announcement files:
 - a. Make sure the Branch Gateway is registered with the Communication Manager.
 - b. On the change media-gateway screen of the Communication Manager SAT interface, set *enable CF* to *y*.
 - c. On the Communication Manager SAT interface, enter `enable announcement-board`.
 - d. The announcement files are copied from internal flash to the compact flash, and the compact flash's yellow CARD IN USE (CF BSY) LED flashes.
4. Use the **show platform mainboard** command to make sure the G430 is working properly and to check the status of the compact flash and RAM memory.

For G430 v1 and v2:

```
MAINBOARD BOARD
-----
Type                : G430
Description          : Avaya Inc., G430 Media Gateway
Serial Number        : 08IS26191007
HW Vintage           : 1
HW Suffix            : A
FW Version           : 42.4.0
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
```

G430 v3 does not have the RAM module:

```
MAINBOARD BOARD
-----
Type                : G430
Description          : Avaya Inc., G430 Media Gateway
Serial Number        : 08IS26191007
HW Vintage           : 3
HW Suffix            : A
FW Version           : 42.4.0
No Fault Messages    : No Fault Messages

COMPACT FLASH MEMORY
-----
Type                : 2.0 GB
Serial Number        : STI1M2a407217197453
Model Number         : STI Flash 8.0.0
Faults               : OK
```

Compact flash memory card removals

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](#) on page 74. You may do this to replace the current compact flash memory card with another one holding a different set of announcements.
- [Replacing a compact flash memory card while retaining The current announcements](#) on page 74. 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](#) on page 75.

Swapping compact flash memory cards

Procedure

1. At the SAT interface of the Communication Manager, 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 (CF BSY) LED associated with the compact flash is not flashing.

 Warning:

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

3. Remove the compact flash memory card.
4. Insert the new compact flash memory card into the compact flash (CMPCT FLSH) slot.
5. At the SAT interface of the Communication Manager, enter **enable announcement-board**.

Replacing a compact flash memory card while retaining the current announcements

Procedure

1. Make sure the yellow CARD IN USE (CF BSY) 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 Branch Gateway may reset, causing all announcement files in the 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

About this task

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.

Procedure

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

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

2. At the SAT interface of the Communication Manager, enter **disable announcement-board**, and then set **enable CF** to **n** on the change media-gateway screen.

! Important:

Ensure the yellow CARD IN USE (CF BSY) LED associated with the compact flash is not flashing.

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

3. Remove the compact flash memory card.
4. Optionally replace the 512 MB RAM card with the 256 MB RAM card.
5. At the SAT interface of the Communication Manager, enter **enable announcement-board**.

6. 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.

7. Restore the announcements from the USB device to internal flash by entering the CLI command **restore usb usb-devicebackup-name announcements-internal-flash**.

 Note:

In FIPS mode, identity certificates are not backed-up nor restored to the USB device and must be downloaded again after the restore operation. In FIPS mode backup performed on the same gateway can be restored but backup performed on non-FIPS mode cannot.

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

8. Attach the blank plate with screws to cover the compact flash (CMPCT FLSH) slot.

Chapter 10: Branch Gateway firmware upgrade

The software that is used to control the Branch Gateway and the media modules installed on the Branch Gateway is called firmware. You can upgrade the firmware on Branch Gateway and media modules using various tools, each suitable for specific type of installation.

Important:

You can upgrade to Release 10.1 Build 42.4.0 and later from Build 38.20.0 or earlier only after installing Release 7.1.0.5 Build 38.21.3. If you download Release 10.2 prior installing the Release 7.1.0.2 and run the **show download software status 10** command, the system displays the following error message:

```
Incompatible software image for this type of device.
```

After installing Release 7.1.0.2, you must enable or disable Avaya Logins before downloading Release 10.2 through CLI or SNMP.

You can enable or disable Avaya Logins by using one of the following options:

1. Use one of the following commands.
 - a. **login authentication services**: To enable Avaya Logins.
 - b. **no login authentication services**: To disable Avaya Logins.
2. Confirm that Avaya Logins can be enabled or disabled during firmware download. If the confirmation was not completed previously, you can confirm this when you download the software using one of the following commands:
 - a. **copy ftp SW_imageA**
 - b. **copy ftp SW_imageB**
 - c. **copy scp SW_imageA**
 - d. **copy scp SW_imageB**
 - e. **copy tftp SW_imageA**
 - f. **copy tftp SW_imageB**
 - g. **copy usb SW_imageA**
 - h. **copy usb SW_imageB**
 - i. **copy https SW_imageA**

- j. `copy https SW_imageB`
- k. `copyedge scp SW_imageA`
- l. `copyedge scp SW_imageB`

If you upgrade Branch Gateway from Release 7.1.0.x Build 38.21.x to Release 7.1.2 Build 39.xx or later (Build 40.xx) the system will prompt to enable or disable EASG.

*** Note:**

In Release 7.1 or later, the gateway defaults to using TLS 1.2, PTLS, and unencrypted H.248 communication with CM. Use the `set link-encryption` command to adjust these settings.

Firmware upgrades using Solution Deployment Manager

You can use Solution Deployment Manager to view your network inventory and the firmware vintages of devices on your network. Solution Deployment 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.

By using Solution Deployment Manager, you can update the software on your devices.

For information about using Solution Deployment Manager, see *Administering Avaya Aura® System Manager*.

*** Note:**

You cannot upgrade G430 v3 using Solution Deployment Manager.

Upgrading firmware using the command line interface through SCP/FTP/TFTP/HTTPS

About this task

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

Procedure

1. Prepare installation worksheets.

See [Preparing installation worksheets](#) on page 80.

2. Set up an SCP, FTP, TFTP, or HTTPS server on the LAN connected to the Branch Gateway.

For information about setting up a file server, see [Setting up a TFTP server](#) on page 81.

If you use an FTP server, the Branch Gateway prompts you for a username and password when you enter a command to transfer a file.

3. Download the firmware files to the SCP, FTP, TFTP, or HTTPS server.

For more information, see [Downloading Branch Gateway firmware files to a local file server](#) on page 81.

4. Run the required CLI commands.

CLI commands for upgrading Branch Gateway firmware via SCP/FTP/TFTP/HTTPS

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

- 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 Branch Gateway firmware into Bank A from an FTP server.
- Use the **copy ftp SW_imageB** command to upgrade the Branch Gateway firmware into Bank B from an FTP 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 Branch Gateway firmware into Bank A from a TFTP server.
- Use the **copy tftp SW_imageB** command to upgrade the Branch Gateway firmware into Bank B from a TFTP server.
- Use the **copy scp module** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from an SCP server.
- Use the **copy scp SW_imageA** command to upgrade the Branch Gateway firmware into Bank A from an SCP server.
- Use the **copy scp SW_imageB** command to upgrade the Branch Gateway firmware into Bank B from an SCP server.
- Use the **copy https module** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from an HTTP or HTTPS server.
- Use the **copy https SW_imageA** command to upgrade the Branch Gateway firmware into Bank A from an HTTP or HTTPS server.

- Use the `copy https SW_imageB` command to upgrade the Branch Gateway firmware into Bank B from an HTTP or HTTPS server.
- Use the `copyedge scp module` command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from an SCP server via Avaya SBC tunnel.
- Use the `copyedge scp SW_imageA` command to upgrade the Branch Gateway firmware into Bank A from an SCP server via Avaya SBC tunnel.
- Use the `copyedge scp SW_imageB` command to upgrade the Branch Gateway firmware into Bank B from an SCP server via Avaya SBC tunnel.

Example upgrade via SCP/FTP/TFTP/HTTPS 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
```

The following example downloads a firmware version with the path and file name `C:\g430_sw_42_4_0.bin.net` from an FTP server with the IP address `149.49.134.153` to Bank A of the Branch Gateway:

```
copy ftp SW_imageA C:\g430_sw_42_4_0.bin 149.49.134.153
```

* Note:

The above specified path is the FTP server directory. Set the boot bank location for the new firmware as per your customized configuration, and reboot the gateway.

See *Avaya Branch Gateway G430 CLI Reference* guide for a list of all commands for the gateway.

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 SCP, FTP, TFTP or HTTPS server, you also need to plan the SCP, FTP, TFTP or HTTPS server IP address, login, and password.

Server Values worksheet

Table 6: Software and firmware upgrade file names

Items for Upgrading	New file name for target
File for LSP and primary controller (not used for individual files)	
Branch Gateway Processor	

Table continues...

Items for Upgrading	New file name for target
Branch Gateway Device Manager	
MM710 E1/T1 media module	
MM710B E1/T1 media module	
MM711 Analog Port 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	
MM721 BRI media module	
MM722 BRI Trunk media module	

File server setup

To load single firmware files on a Branch Gateway, you must put the files on a computer connected to the customer's LAN in the customer's network. You log on to the Branch Gateway later and use the gateway's SCP, FTP, TFTP or HTTPS capability to download the new firmware. Set up a SCP, FTP, TFTP or HTTPS server on the LAN.

Note:

Use a Linux or Unix SCP, FTP, TFTP or HTTPS server only if a Linux or Unix SCP, FTP, TFTP or HTTPS 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 Branch Gateway firmware files to a local file server

Procedure

1. Go to the [Avaya support](#) website.
2. Navigate to Media Gateway downloads.
3. Locate the file names that match the files listed in your installation worksheet.

For sample firmware file names, see [Sample software and firmware file names](#) on page 82.

4. Double-click the file name of the file you want to download.

The File Download window appears.

Downloading files can occasionally add "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 SCP, FTP, TFTP or HTTPS server on the local LAN that was created for this purpose.

For more information, see [Setting up a file server](#) on page 81.

Sample software and firmware file names

Component	File name Example	Notes
Branch Gateway Processors		
Branch Gateway Processor (G430 v1, v2)	<i>g430_sw_42_4_0.bin</i>	G430 hardware vintage 1 and 2 uses the software image <i>g430_sw_x_y_x.bin</i> . For checking the hardware vintage of the model before downloading the G430 software image, see Checking the G430 hardware vintage from the Branch Gateway CLI on page 83.
Branch Gateway Processor (G4G43030 v3)	<i>g430v3_sw_42_4_0.bin</i>	G430 hardware vintage 3 uses the software image <i>g430v3_sw_x_y_x.bin</i> . For checking the hardware vintage of the model before downloading the G430 software image, see Checking the G430 hardware vintage from the Branch Gateway CLI on page 83.
Media modules		
MM710 E1/T1 media module	<i>mm710v3.fdl</i>	
MM710B E1/T1 media module	<i>mm710v3.fdl</i> <i>mm710bv47.fdl</i>	
MM711 Analog Port/Trunk media module (version 6 or earlier)	<i>mm711v16.fdl</i>	
MM711 Analog Port/Trunk media module (version 7)	<i>mm711h7v21.fdl</i>	
MM711 Analog Port/Trunk media module (version 20 or later)	<i>mm711h20v54.fdl</i>	
MM712 DCP media module	<i>mm712v14.fdl</i>	
MM714 Analog Port/Trunk media module	<i>mm714v5.fdl</i>	
MM714B Analog Port/Trunk media module	<i>mm714h10v93.fdl</i>	

Table continues...

Component	File name Example	Notes
MM716 Analog Port/Trunk media module	<i>mm716v80.fdl</i>	
MM717 DCP media module	<i>mm717v3.fdl</i>	
MM720 BRI media module	<i>mm720v1.fdl</i>	
MM721 BRI media module	<i>mm721v1.fdl</i>	
MM722 BRI media module	<i>mm722v3.fdl</i>	

Example failure message if the wrong image is used

The system displays a failure message if a wrong image is used. Run the following command:

```
show download software status 10
```

The system displays the following message:

```
Module #10
=====
Module           : 10
Source file      : g430_39_12_0.bin
Destination file : G430-A
Host             : 135.9.1.75
Running state    : Idle
Failure display  : Incompatible software image for this type of device
Last warning     : No-warning
```

Checking the G430 hardware vintage from the Branch Gateway CLI

About this task

You can check the hardware vintage of the model before downloading the G430 software image.

Procedure

1. Login to the application CLI interface.
2. To check the hardware vintage, run the command:

show system and check the rows **Model** and **HW Vintage**.

- G430 v1 displays the following message:

```
System Name           :
System Location       :
System Contact        :
Uptime (d,h:m:s)     : 1,21:46:21
Call Controller Time  : 13:48:01 09 MAR 2018
```

```
Serial No           : 10IS08355993
Model               : G430
HW Vintage          : 1
HW Suffix           : A
FW Vintage          : 39.5.0
LAN MAC Address     : 00:1b:4f:3c:d2:59
WAN MAC Address     : 00:1b:4f:3c:d2:5b
SERVICES MAC address : 00:1b:4f:3c:d2:58
RAM Memory          : 256MB
Compact Flash Memory : CompactFlash card is disabled
Main PSU            : 175W
POE PSU             : Not present
Media Socket #1     : 25 channels on board VoIP DSP
Media Socket #2     : MP120 VoIP DSP Module
FANS                : No Fault messages
```

- G430 v3 displays the following message:

```
System Name         :
System Location      :
System Contact       :
Uptime (d,h:m:s)    : 0,05:00:45
Call Controller Time : 13:44:33 09 MAR 2018
Serial No           : 170L5120N039
Model               : G430v3
HW Vintage          : 3
HW Suffix           : A
FW Vintage          : 39.11.1
LAN MAC Address     : c8:1f:ea:63:b4:01
WAN MAC Address     : c8:1f:ea:63:b4:03
SERVICES MAC address : c8:1f:ea:63:b4:00
Compact Flash Memory : No CompactFlash card is installed
Main PSU            : 175W
POE PSU             : Not present
Media Socket #1     : 40 channels on board VoIP DSP
Media Socket #2     : Not present
FANS                : No Fault messages
```

 Note:

The G430 v3 displays G430v3 as the Model and 3 as the HW Vintage.

Checking the G430 hardware vintage from the Communication Manager web interface

About this task

You can check the hardware vintage of the model before downloading the G430 software image from the Communication Manager web interface.

Before you begin

Log in to the Communication Manager web interface.

Procedure

To check the hardware vintage, run the following command:

display media-gateway 11 and check the row FW Version/HW Vintage.

The system displays the following message:

```

MEDIA GATEWAY 11

Type: g430
Name: g430v3
Serial No: 170L17201039
Link Encryption Type: any-ptls/tls      Enable CF? y
Mutual Authentication: optional
Network Region: 53                      Location: 1
Use for IP Sync? y                      Site Data:
Recovery Rule: 1

Registered? y
Gateway Mode: Enterprise
FW Version/HW Vintage: 39 .11 .1 /3
MGP IPV4 Address: 172.16.1.206
MGP IPV6 Address: fd00:db3:9:75::206
Controller IP Address: 172.16.1.168
MAC Address: a4:25:1b:aa:0b:0d

Mutual Authentication? optional

```

*** Note:**

The G430v3 displays 3 as the HW Vintage.

Upgrading Branch Gateway firmware using the CLI via a USB device

About this task

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

Procedure

1. Prepare installation worksheets.
See [Preparing installation worksheets](#) on page 80.
2. Download the firmware files to a PC.

See [Downloading Branch Gateway firmware files to a local PC](#) on page 86.

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 the Branch Gateway USB port.
5. Run CLI commands to copy the firmware files from the USB mass storage device to the Branch Gateway.

See [CLI commands for upgrading Branch Gateway firmware via a USB device](#) on page 86.

CLI commands for upgrading Branch Gateway firmware via a USB device

You can use CLI commands to upload an upgrade file from a USB mass storage device to the Branch Gateway. You must use the specific path to the file on the 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 Branch Gateway firmware into Bank A from a USB mass storage device
- Use the `copy usb SW_imageB` command to upgrade the Branch Gateway 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 usbdevice0 \temp\mm712v51.fdl 3
```

Downloading firmware files to a local computer

Procedure

1. Go to the [Avaya support](#) website.
2. Navigate to Media Gateway downloads.
3. Locate the file names that match the files listed in your installation worksheet.

For sample firmware file names, see [Sample software and firmware filenames](#) on page 82.

4. Double-click the file name of the file you want to download.

The File Download window appears.

5. Select **Save this file to disk**.
6. Save the file to a directory on the local computer.

7. **(Optional)** Use WinZip or another zip file tool to unzip the firmware file before copying it to the local computer.

Chapter 11: Upgrading IP phone configuration and firmware files

IP phone configuration and firmware file upgrades

Branch 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 outgoing directory for phone images and scripts.

 Note:

TFTP server support is available only for IPv4.

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

IP phones supported by the local TFTP server feature

The following IP phones are supported by the local TFTP server feature:

- H.323:
 - 4601
 - 4601+
 - 4602
 - 4602SW
 - 4602SW+
 - 4606
 - 4610SW
 - 4612/24
 - 4620
 - 4620SW

- 4621SW
- 4622SW
- 4690
- SIP:
 - 4602 SIP
 - 4602SW
 - 4602SW+
 - 4610SW
 - 4620SW
 - 4621SW

The following IP phones are not supported by the local TFTP server feature:

- 4630
- 4630SW

If you have an S8300 installed on Branch Gateway, you can alternatively upgrade IP phones using the Communication Manager web interface.

The IP address of the TFTP server is the PMI.

CLI commands for upgrading Branch Gateway firmware via SCP

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

- Use the **copy scp module** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from an SCP server
- Use the **copy scp SW_imageA** command to upgrade the Branch Gateway firmware into Bank A from an SCP server
- Use the **copy scp SW_imageB** command to upgrade the Branch Gateway firmware into Bank B from an SCP server

Administering the upgrade

When using supported IP phones with the Branch Gateway, 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.

Related links

[Upgrade administration](#) on page 90

Upgrade administration

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 Branch Gateway.

 Note:

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

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](#) on page 92, otherwise proceed to step [6](#) on page 91.
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 Branch Gateway 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 Branch Gateway 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 Branch Gateway 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 Branch Gateway 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.

Related links

[Administering the upgrade](#) on page 90

TFTP IP telephone upgrade examples

About this task

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.

Related links

[Upgrading 4602SW and 4602D phones](#) on page 92

[Upgrading 4620 IP phones](#) on page 94

Upgrading 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](#) on page 92, otherwise proceed to step [5](#) on page 93.
2. Set the memory size for the image files using the `ip tftp-server file-system size` command.

For example:

```
Gxxx-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
Gxxx-001(super)
```

3. Copy the running configuration to the start-up configuration using the `copy running-config startup-config` command.

For example:

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

4. Reset the Branch Gateway using the **reset** command.

For example:

```
Gxxx-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:

```
Gxxx-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
Gxxx-001(super)#
Gxxx-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
Gxxx-001(super)#
```

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

For example:

```
Gxxx-001(super)# copy ftp phone-imageA pub\4602dbtel_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
Gxxx-001(super)# copy ftp phone-imageB pub\4602sbtel_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:

```
Gxxx-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
Gxxx-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.

Related links

[TFTP IP telephone upgrade examples](#) on page 92

Upgrading 4620 IP phones

Procedure

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

For example:

```
Gxxx-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:

```
Gxxx-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
```

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

Related links

[TFTP IP telephone upgrade examples](#) on page 92

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 7: 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.
"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.

Table continues...

Problem	Possible cause	Action
"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.

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 than 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 12: Branch Gateway backups and restores

This chapter provides instructions for backing up and restoring the Branch Gateway configuration using local backups (USB) and remote backups (network servers). These procedures are important for Branch Gateway replication and restoration after failures.

Backup and restore methods

- Local backup: Use a USB mass storage device with the **backup config usb** and **restore usb** CLI commands. The local backup method is the most efficient way to restore the Branch Gateway.
- Remote backup: For the remote Branch Gateway, backup and restore individual files using the TFTP, FTP, SCP, or HTTPS server.

The **backup config usb** command saves the gateway configuration, announcement files, TLS certificates, and special VoIP parameters to a USB drive. You can use the USB drive to restore the files to a previously known good state.

Best practices for backup

- Before you perform a backup, run the **copy running-config startup-config** command. This action ensures that the backup includes the current running configuration and allows you to check whether the configuration uses the default password.
- Insert the USB drive into a gateway USB port and run the following command to verify that the Branch Gateway detects the USB drive formatted as FAT16 or FAT32: **show usb all**
- Run the following command to list the directory contents: **dir usbdevice [directory]**
- When performing the backup, run the **show system** command to determine whether the gateway uses a Compact Flash to store announcements. If the gateway does not use Compact Flash, the Compact Flash Memory status displays `not installed` or `disabled`. You need this information when restoring a new gateway from a USB drive if the gateway is not yet registered to Communication Manager.
- Verify the software load in the **show system** command output. To restore the complete configuration to a new board, ensure that the software load is the same or newer. If the software load is older, Branch Gateway does not support certain features and might ignore their configurations. Store the downloadable software image in the USB drive backup directory.

- Run the **show fips-mode** command to determine the FIPS mode status.
- Before extracting the USB drive from the gateway, run the **safe-removal usb usbdevice0** command to prevent Branch Gateway file corruption.

*** Note:**

Maintain current backups to avoid using out-of-date data during a restore. When creating a backup directory, consider including the backup date in the directory name. If you restore a configuration that contains old, forgotten user passwords, you cannot log in. To resolve this, you must perform a manual `nvrw init` operation using the dedicated jumper on the gateway.

Backup and restore operations

About this task

You can use this procedure for both FIPS and non-FIPS mode gateways when restoring to the same or a different gateway. Restoring to a different gateway requires additional considerations.

*** Note:**

For non-FIPS mode gateways, if you update the configuration master key after performing a backup, the restore operation fails. In this scenario, create a new backup immediately after updating the configuration master key. You cannot update the configuration master key in FIPS mode gateways.

Backing up G430 gateway

Procedure

1. Insert the USB drive and run the following command to see its content:

```
dir usbdevice
```

2. Run the following backup command:

```
backup config usb usbdevice0 <backup-dir>
```

If the gateway is not registered to Communication Manager you need also to specify whether the announcements are saved to internal flash or compact flash memory.

For example:

```
g430-007(super)# backup config usb usbdevice0 g430-007_2025-01-15
Backup operation will copy existing files on the gateway to usb mass storage
device.
Do not remove USB device until the end of operation.
Do you want to continue (Y/N)? y
Beginning backup operation ...
```

```
This operation may take a few minutes ...
Please refrain from any other operation during this time.
For more information, use 'show backup status' command.
g430-007(super)# show backup status
```

Backup operation was successful.

Files backup:

Type	FileName	Status
startup-config	/usb0/g430-007_2025-01-15/startup_config.cfg	OK
announcement	/usb0/g430-007_2025-01-15/GWANNC/anncl.wav	OK
announcement	/usb0/g430-007_2025-01-15/GWANNC/annc2.wav	OK
...		
other	/usb0/g430-007_2025-01-15/audio8122.bin	OK
other	/usb0/g430-007_2025-01-15/trust/easg/productId	OK
other	/usb0/g430-007_2025-01-15/trust/easg/confirmation	OK
other	/usb0/g430-007_2025-01-15/trust/easg/state	OK
etc...		

Restoring a gateway backup

Procedure

1. Insert the USB drive and run the following command to see its content:

```
dir usbdevice
```

2. Run the following command where the backup was saved:

```
restore usb usbdevice0
```

If the gateway is not registered to the Communication Manager, you must specify the announcements location using one of the following commands:

- **announcements-internal-flash**
- **announcements-compact-flash**

For example:

```
G430-??? (super)# restore usb usbdevice0 <backup-dir> announcements-internal-flash
Restore operation will remove existing files on the gateway. Do not remove
USB device until the end of operation.
Do you want to continue (Y/N)? y
```

```
Initializing announcement file system - this may take a few minutes.
Beginning restore operation ...
This operation may take a few minutes ...
Please refrain from any other operation during this time.
For more information, use 'show restore status' command.
```

The gateway resets during the restore operation. You can check the current status of the restore both before and after the reset. After the reset, the passwords saved at the time of the backup are restored.

3. To check the final status of the restore operation after the reset, run the following command:

show restore status

For example:

```
g430-007(super)# show restore status

Restore operation was successful.
Files restored:
Type                FileName                Status
-----
announcement        Announcement files      OK
startup-config       startup_config.cfg      OK
other                audio8122.bin           OK
other                trust                   OK
other                easg                    OK
other                CA                       OK
other                productID               OK
other                confirmation             OK
other                state                    OK
etc..
```

4. Reinstall the TLS gateway certificates using the following command:

```
copy scp/usb gw-identity-cert
```

 Warning:

In FIPS mode, the TLS gateway identity certificates are not restored and must be downloaded again manually after the restore operation is completed.

For example:

```
G430-??? (super)# restore usb usbdevice0 g430-backup announcements-internal-
flash
Restore operation will remove existing files on the gateway. Do not remove USB
device until the end of operation.
Do you want to continue (Y/N)? y

In FIPS mode the gateway identity certificates/keys are not restored.
You must reinstall them using the 'copy scp/usb gw-identity-cert' commands.
Do you want to continue (Y/N)? y
```

 Warning:

You cannot restore to a FIPS mode gateway if the gateway enters (or re-enters) FIPS mode after the backup.

Preserving SNMP engine ID

About this task

Perform this procedure only if you want to preserve the same SNMP engine ID to use it after you replace the gateway. By default, the gateway derives the SNMP engine ID from the gateway's MAC address.

Procedure

1. Record the old engine ID using the following command:
2. Save the old engine ID to the new gateway using the following command:

```
show snmp engineID
```

```
snmp-server engineID <engineID>
```

Backup and restore for G430 gateway replacement

The backup and restore process depends on the gateway's FIPS mode status. Determine the current mode using the `show fips-mode` command.

Backing up and restoring for non-FIPS mode gateways

About this task

The standard backup and restore procedure works as expected, provided the configuration master key on the old gateway matches the new gateway.

Procedure

1. On the old gateway, run the following command to verify the master key:

```
copy running-config startup-config
```

If the command prints the warning, the backup from the old gateway can be restored on the new gateway without any further action.

For example:

```
Warning! It is a recommended policy to override default configuration master key
with user defined secret - for details see user reference.
```

If the command does not print the warning, the user has configured a new master configuration key.

2. **(Optional)** If you do not know the master configuration key, do the following:
 - a. Set a new passphrase. Run the following command:


```
key config-key password-encryption
```
 - b. Save the passphrase. Run the following command:


```
copy running-config startup-config
```
3. After changing the key, record the new passphrase and perform the backup of the old board.
4. Insert the new board and enter the default username `root` and password `root` to log in.
5. Change the password and configure EASG.

The following are the options:

- Enable
- Disable

6. **(Optional)** If you are restoring from a backup, you can skip the initial gateway configuration and disable DHCP.

For example:

```
--- Gateway Configuration Script ---
The script will provide you basic gateway connectivity configuration.
Configuration Script - do you want to continue (Y/N)? n

Note: The PMI is currently configured with DHCP on VLAN 1
Do you want to remove it [Y]: y
```

If you configured a master configuration key password before the backup, you must set the same configuration password for the new gateway using the following commands:

- **key config-key password-encryption**
- **copy running startup-config**

7. To check the software load, run the following command:

show system

After the backup is done, if the software load is older than the one used in the previous gateway, then:

- Update the software load manually. You can update the software using an image stored in the USB drive so you do not need to configure the networking parameters.
- Allow the restore operation update the software load. If you manually add software downloadable files to the backup directories, the restore also updates the firmware of the gateway and media modules. The gateway software must be present in the backup folder, and the media module firmware must be present in the MM subfolder.

For example:

A backup directory that contains a G430v3 software image version 43.28.0.

```
g430-???(super)# dir usbdevice0 g430-backup
      Date                Type                Size(Bytes)                Filename
      -----
2026-01-15,11:17:48      file                      728                      audio8122.bin
2026-01-15,11:17:48      file                      865                      README.TXT
2026-01-15,15:09:38      file                    16598907                  g430v3_sw_43_28_0.bin
2026-01-15,11:17:46      <DIR>                     4096                      IPPHONE
2026-01-15,11:17:48      <DIR>                     4096                      GWANNC
2026-01-15,11:17:46      <DIR>                     4096                      MM
2026-01-15,11:17:48      <DIR>                     4096                      TRUST
2026-01-15,16:18:34      file                      2038                      startup_config.cfg
```

8. Restore the USB backup to the new board. See [Restoring a gateway backup](#) on page 99.

For example:

A software update during the restore operation, before the automatic reset.

```
g430-???(super)# show restore status
Restore operation in progress.
```

```
Files restored:
Type              FileName              Status
-----
startup-config    startup_config.cfg    OK
announcement      anncl.wav             OK
announcement      anncl2.wav            OK
swComponent       g430v3_sw_43_28_0.bin Copying...
```

9. Update the gateway serial number in Communication Manager using the value displayed in the **show system** command output. Run the following command:

```
change media-gateway <n>
```

Backing up and restoring for FIPS mode gateways

About this task

FIPS mode gateways use a secure configuration key that cannot be modified and it is different for each gateway.

Procedure

1. Insert the new board and enter the default username `root` and password `root` to log in.
2. Change the password and configure EASG.

The following are the options:

- Enable
- Disable

3. **(Optional)** If you are restoring from a backup, you can skip the initial gateway configuration and disable DHCP.

For example:

```
--- Gateway Configuration Script ---
The script will provide you basic gateway connectivity configuration.
Configuration Script - do you want to continue (Y/N)? n

Note: The PMI is currently configured with DHCP on VLAN 1
Do you want to remove it [Y]: y
```

4. Configure the gateway for FIPS mode of operations using the following command:

```
set fips-mode enable
```

The gateway will reset.

In FIPS mode, you can only restore from a backup that was performed on the same gateway. The restore command fails if executed on a different gateway.

For example:

```
G430-??? (super) # show restore status
Last restore failed with error: genError(2) - Error 210 during download file
/usb0//g430na-nofips/startup_config.cfg: Failed Saving Line 4. The
configuration file was encrypted with a different key. Configuration download
operation was aborted.
```

5. To restore non-security data, manually remove all `encrypted-*` lines by editing the configuration stored in the backup file: `startup_config.cfg`
6. Restore the USB backup to the new board. See [Restoring a gateway backup](#) on page 99.

Username, SNMPv3 users, TLS identity certificates must be manually reloaded to the new gateway, even if it appears that they are restored. If you use this method of restoring non-security data after the automatic reset is performed by the restore you need to log in again using the default password.

7. Configure the password and save the configuration with the new password. Run the following command:

```
copy running-config startup-config
```

At the time of the backup, you need to list the usernames and the SNMPv3 users using the `show usernames` and `show snmp user` command respectively and remember to restore them after the restore operation is completed. You can run the `show gw-identity h248reg|sla|syslog|web` command to verify which certificates are present and should be restored.

8. Update the gateway serial number in Communication Manager using the value displayed in the `show system` command output. Run the following command:

```
change media-gateway <n>
```

Gateway replacement checklist

Non-FIPS mode gateway replacement checklist

Step	Procedure/Action	CLI command/Note
Pre-replacement (backup procedure)		
Save running config	Required: Save the current running configuration.	<code>copy running-config startup-config</code>
Check for default master key	Run <code>copy running-config startup-config</code> . If no warning is printed, a non-default key is configured, proceed to step 3 if not known. If a warning is printed, proceed to step 4.	<code>copy running-config startup-config</code>  Note: Look for the Warning! It is a recommended policy... message.

Table continues...

Step	Procedure/Action	CLI command/Note
Set master key (if non-default)	If a non-default master key was configured (no warning in step 2) and the key is unknown, set a new passphrase before performing the backup.	key config-key password-encryption followed by copy running-config startup-config
Check announcements location and SW load	Required. Record the current load version and the announcement storage location (Compact flash or Internal).	show system To see announcement files: show announcements files brief
Record SNMP Engine ID	Recommended. Record the current SNMP Engine ID to maintain it on the new board.	show snmp engineID
Perform backup	Required. Perform the backup to a directory on the USB drive.	backup config usb usbdevice0 <backup-dir> If the gateway is not registered, add announcement location.
Safe removal	Required. Safely remove the USB drive.	safe-removal usb usbdevice
Post-replacement (restore procedure)		
Initial new board login	Login with default credentials (root, root), answer the EASG question, skip the configuration script, and disable DHCP.	Respond n to Configuration Script and y to remove DHCP.
Set master key (if non-default)	If a master key was configured on the old board (step I.3), set the same key on the new board before restoring.	key config-key password-encryption followed by copy running startup-config
Update software load	Check and update. If the new board's software load is older than the backup's, update it manually or include the software image in the backup folder for automatic update during restore.	show system to check; place g430v3_sw_...bin in backup directory for automatic software update during the restore.
Restore from USB	Standard procedure.	restore usb usbdevice0 <backup-dir> [announcements-location]
Restore SNMP Engine ID	If needed. Set the old SNMP Engine ID.	snmp-server engineID <engineID> (using the value recorded in Step I.5)

FIPS mode gateway replacement checklist

Step	Procedure/Action	CLI command/Note
Pre-replacement (backup procedure)		
Save running config	Required. Save the current running configuration.	<code>copy running-config startup-config</code>
Record security info	Required. Configuration master key cannot be modified in FIPS mode, so certain security-related data is not restored. Record the necessary information.	• <code>show usernames</code> • <code>show snmp user</code> • <code>show gw-identity h248reg syslog..</code>
Check announcements location and SW load	Required. Record the current load version and the announcement storage location (Compact flash or Internal).	<code>show system</code> To see announcement files: <code>show announcements files brief</code>
Record SNMP Engine ID	Recommended. Record the current SNMP Engine ID to maintain it on the new board.	<code>show snmp engineID</code>
Perform backup	Required. Perform the backup to a directory on the USB drive.	<code>backup config usb usbdevice0 <backup-dir></code>
Safe removal	Required. Safely remove the USB drive.	<code>safe-removal usb usbdevice</code>
Post-replacement (restore procedure)		
Initial new board login	Login with default credentials (root, root), answer EASG questions, skip the configuration script, and disable DHCP.	Respond <code>n</code> to configuration script and <code>y</code> to remove DHCP.
Enable FIPS mode	Required. Configure the gateway for FIPS mode. The gateway will reset, and you must repeat step II.1 afterward.	<code>set fips-mode enable</code>
Update software load	Check and update. If the new board's software load is older than the backup's, update it manually or include the software image in the backup folder for automatic update during restore.	<code>show system</code> to check; place downloadable image. <code>g430v3_sw_...bin</code> in backup directory for automatic software update during the restore.
Manual configuration to restore non secure data	Recommended. Manually edit <code>startup_config.cfg</code> on the USB drive to remove all <code>encrypted-*</code> lines.	Edit the <code>startup_config.cfg</code> and remove all <code>encrypted-*</code> lines.

Table continues...

Step	Procedure/Action	CLI command/Note
Restore from USB	Restore will fail if step 5 was not done due to the secure configuration key mismatch (keys are unique to each gateway).	<code>restore usb usbdevice0 <backup-dir> [announcements-location]</code>
Manual password/config Save	Required. After the restore, login with the default password, configure a new password, and save the configuration.	<code>copy running-config startup-config</code>
Restore recorded security info	Required. Manually reload the usernames, SNMPv3 users, and TLS certificates that were recorded in step 1.2.	<code>username snmp username</code> <code>copy scp/usb gw-identity-cert</code> commands for certificates.
Restore SNMP Engine ID	If needed. Set the old SNMP Engine ID.	<code>snmp-server engineID <engineID></code> (using the value recorded in Step 1.3).

Post restoration of gateway checks

Useful commands to verify the restoration and gateway status.

- `show running-config`
- `show announcements files brief`
- `show voip-parameters`
- `show gw-identity-cert [h248 | syslog | sla | web]`
- `show root-ca [h248 | syslog | sla | web]`

Chapter 13: Troubleshooting

You can have problems with phones, a trunk, the power, or the WAN. 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 Branch 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

Proposed Solution

Procedure

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. For more information, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*

No power on the Branch Gateway

Proposed Solution

Procedure

1. Check the AC power source with a voltmeter.

2. Connect the Branch Gateway to a different AC power source.

If the Branch Gateway has power, the problem is with the original power source. If the Branch Gateway still does not work, go on to the next step.

3. Check the ALM LED on the Branch Gateway chassis.

If it is lit, there may be a system-wide problem. Contact your project manager. See “Front panel description”.

CLI is not accessible

Check the connectivity to the Branch Gateway. Correct the ip address and subnet on the PC attached to the Branch Gateway, 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 Branch Gateway, for example when the Branch Gateway resets continuously.

 Important:

Performing the NVRAM Init restores the Branch Gateway to its initial state with the default settings.

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

 Voltage:

Disconnect the Branch Gateway 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.

Proposed Solution

Procedure

1. Remove the Branch Gateway cover.
2. Locate the NVRAM init jumper (jumper J3801 for G430 v1 and v2 and jumper J701 for G430 v3) on the front of the Branch Gateway motherboard.

Refer to the figures below. Note that the jumper's two pins closest to the rear of the G430 are bridged.

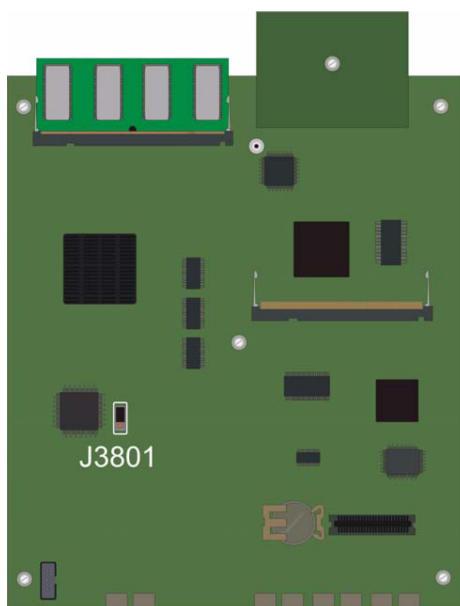


Figure 22: Branch Gateway G430 v1 and v2 NVRAM INIT J3801 Jumper Location



Figure 23: Branch Gateway G430 v3 NVRAM INIT J701 Jumper Location

3. Move the bridge on jumper J3801 so the two pins closest to the front of the G430 are bridged.
4. Put the G430 cover back on the unit, and attach 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 Branch Gateway 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. Remove the top cover screw, and remove the Branch Gateway 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 Branch Gateway will continue to initialize the NVRAM when it resets or is powered up.

12. Install the Branch Gateway cover.

Chapter 14: Front panel description

You can use the front panel of the Branch Gateway to:

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

The front panel of the Branch Gateway chassis without media modules

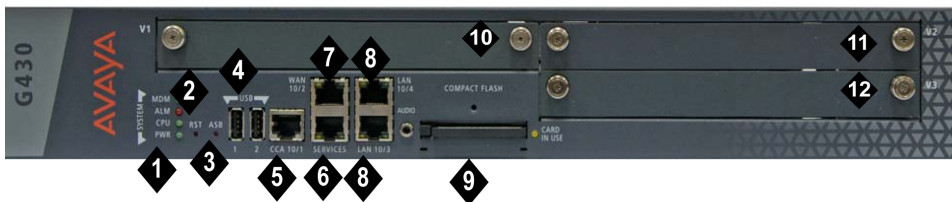


Figure 24: The G430 front panel ports and slots

- | | |
|---------------------------------|---|
| 1. System (SYSTM) LEDs | 7. 10/100M ETH WAN port |
| 2. RST button | 8. 10/100M ETH LAN ports (10/100/1000 in G430 hardware vintage 3) |
| 3. ASB button | 9. Compact Flash (CMPCT FLSH) slot |
| 4. USB 2.0 ports | 10. V1: slot for a media module or S8300 Server |
| 5. CCA (Contact Closure) port | 11. V2: slot for a media module |
| 6. 10/100M Services (SVCS) port | 12. V3: slot for a media module |



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

Figure 25: 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 *Slot Allocation*.

System (SYSTM) LEDs

Table 8: Branch Gateway 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 9: 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
ALM	Alarm	Red	An alarm is present in the system
PWR	Power	Green	OFF — No power BLINKING — Problem with power ON — Normal operation

USB ports

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

- USB flash drive
- USB modem

Console port (Console/CNSL)

The Console port is a standard RJ-45 network port. Use the Console port to connect a console device or modem to the Branch Gateway.

 Note:

Use the provided console cable.

Services port (Services/SVCS)

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 Branch Gateway for configuration purposes.

 Note:

Use a cross-over Ethernet cable.

Compact Flash (CMPCT FLSH) Interface

The compact flash slot enables to increase the number of announcement files on the Branch Gateway from 256 to 1024, by storing them on a removable 1 GB compact flash memory card. Note that, since the announcements are played from the RAM, you must also increase the 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 Branch Gateways*, 03-603203.

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

Table 10: Compact Flash CARD IS USE LED states

LED	State	Meaning
CARD IN USE (CF BSY)	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 or is not in use.

The Emergency Transfer Relay (ETR) port

The Emergency Transfer Relay (ETR) port is a standard RJ-45 network port. Use the ETR port to connect to up to two 808A Emergency Transfer Panels. These panels provide basic telephone services in the event of system failure.

When the Emergency Transfer Relay (ETR) feature is activated, the green ETR LED is lit.

For more information on Emergency Transfer Relay, see *Installing an 808A Emergency Transfer Panel and associated telephones*.

For information on installing the 808A Emergency Transfer Panel, see *808A Emergency Transfer Panel Installation Instructions*, which ships with the Emergency Transfer Panel.

Contact Closure (CCA) port

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 Branch Gateway'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 [Installing the Avaya Partner Contact Closure Adjunct](#) on page 51.

Implementing the Contact Closure feature

About this task

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 Branch Gateway 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 (10/100/1000 for G430 hardware vintage 3). You can connect an external LAN to ETH LAN.

RST and ASB buttons

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

The Branch Gateway has two firmware banks:

- Bank A
- Bank B

Each firmware bank contains a version of the Branch Gateway 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 Branch Gateway using the other version. This is particularly important when uploading new versions.

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

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

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

Procedure

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. This information also applies to the MM710.

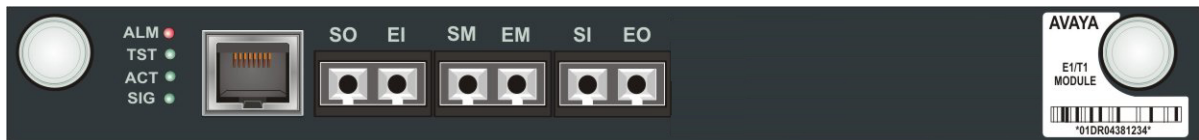


Figure 26: The MM710B media module front panel

* Note:

You can use the six ports in the middle of the front panel for testing.
For drop and insert, you need an external CSU.

MM710B ports

The MM710B contains an E1/T1 port.

MM710B LEDs

Table 11: 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 Branch Gateway. 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 Branch Gateway 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 Branch Gateway 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.

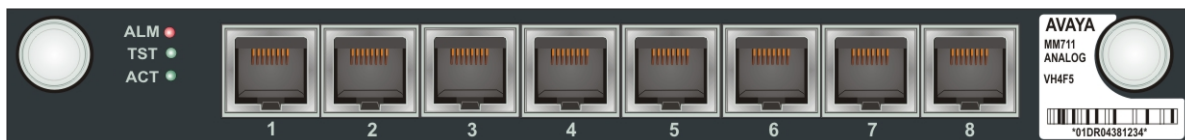


Figure 27: The MM711 media module front panel

MM711 ports

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

MM711 LEDs

Table 12: 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 28: The MM712 media module front panel

MM712 ports

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

MM712 LEDs

Table 13: 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 29: 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 14: 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.

Related links

[The front panel of the Avaya MM714 media module](#) on page 120

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](#) on page 120), 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 30: 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 15: 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.
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 Branch Gateway or if the Branch Gateway becomes unregistered from its Media Gateway Controller (MGC). Turning on ETR manually using the <code>set etr manual-on</code> CLI command also lights this LED.

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 Communication Manager version 2.0 and higher, and Branch Gateway firmware version 25.0.0 and higher.



Figure 31: 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 16: 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
21	Violet	Blue

Table continues...

Station port	Cable pair	
22	Violet	Orange
23	Violet	Green
24	Violet	Brown
OPEN	Violet	Slate

MM716 LEDs

Table 17: 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 32: 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 18: 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
21	Violet	Blue
22	Violet	Orange
23	Violet	Green
24	Violet	Brown
OPEN	Violet	Slate

MM717 LEDs

Table 19: 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 33: The MM720 media module front panel

MM720 ports

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

MM720 LEDs

Table 20: 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 Communication Manager 3.0 or higher, the LED could alternatively indicate that a telephone connected to the module is in use.

Front panel of the MM721 media module



MM721 media module ports

The MM721 has eight ports that are labeled from one to eight. The MM721 ports support the use of a 4-wire BRI station device (TE) when you administer the ports as BRI stations.

MM721 media module LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not configured in the MSG for the slot.
TST	Test	Green	The system performs a test on the module through the server, or the module performs a test on initial insertion.
ACT	Activity	Yellow	A trunk 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.

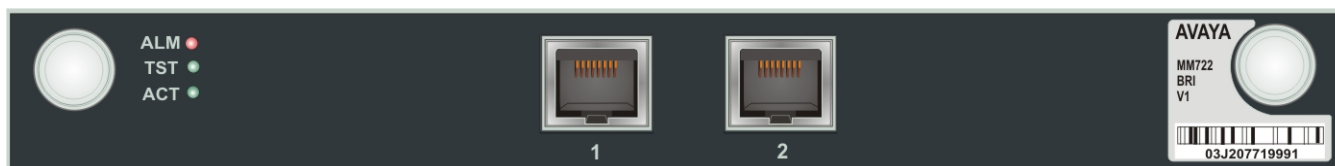


Figure 34: The MM722 media module front panel

MM722 ports

The MM722 contains two ISDN BRI ports.

MM722 LEDs

Table 21: 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 Communication Manager 3.0 or higher, the LED could alternatively indicate that a telephone connected to the module is in use.

Chapter 15: Technical specifications

This section provides technical specifications for the Branch Gateway, for the EM200, for compatible power cords, and for USB modem support.

Specifications

The following table describes the Branch Gateway's physical dimensions and tolerances:

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	5.58 kg
Weight of chassis with the basic configuration, including a 8300 blade server and two media modules	7.45 kg
Ambient working temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10 to 90% relative humidity, non-condensing
Storage temperature	–40°F to 150°F (–40°C to 66°C)
Storage relative humidity	10 to 90% relative humidity, non-condensing
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
Voltage	90 to 264 V AC, 48 to 63 Hz
Power rating	800 BTU/h (234 W)
Max current	2.4 A

EM200 specifications

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

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)
Operating relative humidity	10-90% relative humidity, non-condensing
Storage temperature	-40° to 150°F (-40° to 66°C)
Storage relative humidity	10-90% relative humidity, non-condensing
Operation altitude	up to 10,000 ft (3000 m)
Front Clearance	12 in (30 cm)
Rear Clearance	18 in (45 cm)
Power rating	90V-264V AC, 48-62 Hz
BTU	430 BTU/h
Max current	3 A

Power cord specifications

Following are the specifications for power cords suitable for use with the Branch Gateway:

North America:

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

Outside North America:

The cord must be VDE Certified or Harmonized (HAR), rated 250 V, 3-conductor (3rd wire ground), 1.0 mm² minimum conductor size. Terminate the code at one end to a VDE Certified/CE Marked IEC 60320, sheet C13 type connector rated 10 A, 250 V and the other end to a 3-conductor grounding-type attachment plug rated at a minimum of 10 A, 250 V and a configuration

specific for the region/country in which it is used. The attachment plug must bear the safety agency certification mark(s) for the region/country of installation.

USB modems supported by the Branch Gateway

- 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

Chapter 16: 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 132
- [Call Center](#) on page 132

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 [the figure](#) on page 131.

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

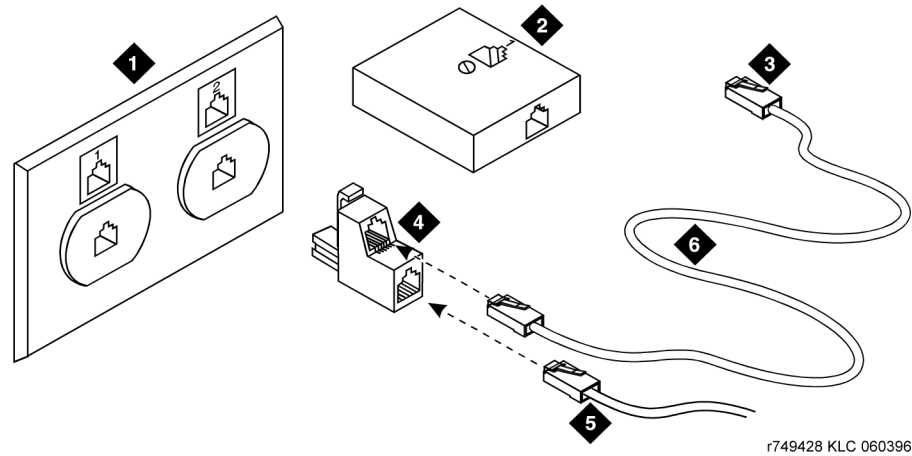


Figure 35: 400B2 Adapter Connecting to a Modular Plug

Table 22: 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

The figure shows typical connection locations for adjunct power.

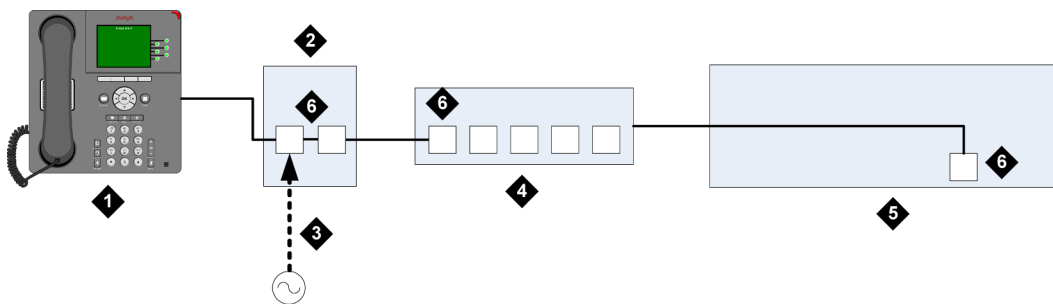


Figure 36: Example Adjunct Power Connections

Table 23: Figure notes:

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

Avaya Aura[®] Communication Manager Messaging application

The Avaya Aura[®] Communication Manager Messaging application runs as a process on the S8300 server. Without the need for additional hardware, the software processes touch-tones, converts messages to the G.711 format, and converts text to speech.

Call Center

An S8300 server provides an excellent solution for a small Call Center. An S8300 server with one or more Branch Gateway supports the following Call Center capabilities:

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

About Avaya Branch Gateway announcement software

Voice announcements are used in a call center environment to announce delays, direct customers to different departments, and inform calling parties. The announcement capability is standard and comes co-resident on the Branch Gateway. You can substantially increase the number of supported announcement files on the Branch Gateway if you install a compact flash and increased RAM. See *Job Aid: Installing the upgrade memory kit*.

Chapter 17: Information checklists

You can use this appendix as an aid for collecting necessary information for the installation of a Branch Gateway.

The following lists are provided:

- [Installer's checklist](#) on page 133: Tools, software, laptop settings, customer network information
- Login information: Serial number of the Branch Gateway and login/passwords for various access methods
- [Quick setup for Media Gateway Processor \(MGP\)](#) on page 134: IP addresses and setup commands for the MGP
- [Installation site information](#) on page 136: Customer and site contact information

Installation checklist

<i>Tools</i>	√
Laptop	
Ethernet interface	
cross-over Ethernet cables	
direct Ethernet cable	
USB flash drive (optional)	
screwdriver	
<i>Software</i>	
Windows operating system	
FTP server program. TFTP server program and SCP server program are recommended	
SSH program	
terminal emulation program: HyperTerminal or other	
TCP/IP networking software: bundled with Windows OS	
web browser: Netscape or Internet Explorer	

Table continues...

<i>Ethernet connections</i>
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 control
<i>SSO login</i>
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.
<i>Dial plan</i>
<i>IP addressing plan</i>
<i>List of customer-provided IP services</i>

Serial number and login information

Logins

Entity	Name & Password
S8300 Server	
Branch Gateway	
SSO Authentication Login	
ftp	anonymous
	email address
Communication Manager	

Quick setup for Branch 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	

Table continues...

Task	CLI Command	Requested Fields	Information to enter
	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	
		<i>module number</i>	
		<i>port number</i>	
Define the CLI prompt	hostname	hostname	
Define a default gateway	ip default-gateway	gateway IP address	
Create a list of validMedia Gateway Controller(s)	set mgc list	IP address1	
		IP address2	
		IP address3	
		IP address4	
An H.248 TLS connection is required	copy scp usb https root-ca h248 reg	File location	Install trusted certificates
Display device information	show system		
Display the current firmware and boot bank information.	show image version		

Installation site information

Site Name	Main Phone
Installation Address	
Shipping Address	
Customer Contact	Name: Title: Phone: Fax: Mobile: Pager: E-mail: Off-hours contact:
Sales person/ Account Executive	Sales/AE phone: Other Contact Info:

Notes to installer: access procedures, safety/security procedures

Access Contact	Name: Title: Phone: Fax: Mobile: Pager: E-mail: Off-hours contact:
Installer Name: Date of Installation:	

Chapter 18: Equipment list

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

*** Note:**

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

Table 24: Equipment List: G430

G430		
The G430 Branch Gateway is a 19-inch 1.5U rack-mountable device. The Branch Gateway contains VoIP resources, a layer 2 switch, modular interface connectivity for traditional trunk and station access, and performs the function of a gateway or gatekeeper. It also houses three Media Module bays, and can be extended to provide up to seven Media Module bays. The Branch Gateway is designed to offer options and scalability. You can mix and match media modules, as well as add additional Branch Gateways as they grow in size.		
G430 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)
700179526	1	Documentation, CIB 3246 FCC/Safety Branch Gateway
700236680	1	Grounding Kit for multiple G430 devices in a 19 inch rack
G430 Comcodes for Customer and Services ordering		

Table continues...

Comcode		Description
700432503		80 channels DSP daughterboard
700432511		20 channels DSP daughterboard
700460660		10 channels DSP daughterboard
700469273		G430 Chassis
700457013		Upgrade memory kit

Table 25: Equipment List: EM200 Expansion Module

EM200 Expansion Module		
The EM200 Expansion Module is a 19-inch 1.5U rack-mountable device. The EM200 contains two Media Module bays, and serves as an extension to the Branch Gateway. You can connect up to two EM200 modules to a Branch 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
700179526	1	Documentation, CIB 3246 FCC/Safety EM200
700236680	1	Grounding Kit for multiple EM200 modules in a 19 inch rack

Table 26: Equipment List: Avaya S8300E server

Server
<i>S8300E server</i>
The Avaya S8300E server is an Intel™-based server complex that carry: • Administration and maintenance provisioning software • Web server • Linux OS • H.248 Branch Gateway Signaling Protocol • CCMS messages tunneled over H.248 Signaling Protocol

Table continues...

Server
The S8300E server can act as the primary server of the Branch Gateway, or can serve as a local survivable processor for remote or branch customer locations.
Comcode (for Services Ordering only): 700407810
Comcodes for S8300E: 700508955,700508924

Table 27: Equipment List: Media Modules

Media Modules		
MM710B T1/E1 Media Module	Comcodes (for Services Ordering Only): 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. MM710B is RoHS compliant.		
DEF DS1 LOOPBACK JACK 700A		
Provides the ability to remotely troubleshoot the MM 710 T1/E1 media module. It is required for any customer with a maintenance contract and highly recommended for any other customer.		
Material Code: 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 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. MM711 is RoHS compliant.		
MM714B Analog Media Module	Comcodes (for Services Ordering Only): 700453889, 700466618	

Table continues...

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 associated with the ports labeled “Line” and not “Trunk”. 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 Branch Gateway supplies only +5 VDC and –48 VDC to the MM712 media module. Any other required voltages must be derived on the module. The MM712 comes with loop range secondary protection. The MM712 is also self-protecting from an over current condition on a tip and ring interface. 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 wink-start or immediate-start. The 24 ports are provided through a 25-pair RJ21X amphenol connector, which can be connected by an amphenol cable to a breakout box or punch down block. MM716 is RoHS compliant.	
MM717 24 port DCP Media Module	Comcode (for Services Ordering Only): 700394711, 700501048
The MM717 DCP Media Module supports 24 DCP stations. The MM717 uses a 25-pair amphenol connector on the media module’s faceplate. The 24 DCP ports are intended for in-building use only. Phone lines connected to those ports are not to be routed out-of-building. Failure to comply with this restriction could cause harm to personnel or equipment. MM717 is RoHS compliant.	
MM720 BRI Media Module	Comcode (for Services Ordering Only): 700394752
The MM720 BRI media module contains eight ports that you can administer 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 does not 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 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.	

Table continues...

Media Modules	
MM720 is RoHS compliant.	
MM721 BRI Media Module	Comcode (for Services Ordering Only): 700393762
The MM721 BRI media module contains eight ports that you can administer 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 does not 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 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. 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 with the central office at the ISDN T reference point. Information is communicated in the same manner as the MM720. MM722 is RoHS compliant.	

Chapter 19: Resources

Branch Gateway documentation

The following table lists the documents related to Branch Gateway. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Description	Audience
Installing and implementing		
<i>Quick Start for Hardware Installation: Avaya G430 Branch Gateway</i>	Describes how to install G430 Branch Gateway in the basic configuration.	Solution architects, implementation engineers, and support personnel
<i>Deploying and Upgrading Avaya G430 Branch Gateway</i>	Describes how to install and upgrade G430 Branch Gateway, perform basic configuration tasks, insert media modules, and connect external devices.	Solution architects, implementation engineers, and support personnel
Administering		
<i>Administering Avaya G430 Branch Gateway</i>	Describes how to configure and manage G430 Branch Gateway after the installation. Contains the detailed information about G430 Branch Gateway features and their implementation.	Solution architects, implementation engineers, and support personnel
<i>Avaya Branch Gateway G430 CLI Reference</i>	Describes the CLI commands for G430 Branch Gateway configuration.	Solution architects, implementation engineers, and support personnel
<i>Avaya Aura® G430 Gateway Data Privacy Guidelines</i>	Describes how to administer G430 Branch Gateway to fulfill Data Privacy requirements.	Solution architects, implementation engineers, and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.

4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Select Release**, select the appropriate release number.

For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.

9. Press **Enter**.

Accessing the port matrix document

Procedure

1. Go to <https://support.avaya.com>.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Choose Release**, select the required release number.
9. In the **Content Type** filter, select one or both the following categories:
 - **Application & Technical Notes**
 - **Design, Development & System Mgt**

The list displays the product-specific Port Matrix document.

10. Press **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at <https://documentation.avaya.com>.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites > Support** on the top menu to open <https://support.avaya.com>.

Using the Avaya Documentation Center, you can:

- Search for keywords.

To filter by product, click **Filters** and select a product.

- Search for documents.

From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** (🌐) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** (☆).

Navigate to the **Manage Content > My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
- Add topics from various documents to a collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon (👁).

Navigate to the **Manage Content > Watchlist** menu, and do the following:

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

 Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Training

The following courses are available on <https://www.avaya-learning.com>. To search for the course, in the **Search** field, enter the course code and click **Go**.

Course code	Course title
20980W	What's New with Avaya Aura®

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at <https://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Index

A

accessing port matrix	143
accessories box	25
adding to	59 , 61
Adjunct	
power connections	130
after installation	57
After installation	
testing	56 , 57
Alternate Software Bank button	116
amphenol cable	
attaching to MM716 and MM717	48
analog	
trunk	61
analog DID	
connecting	46
analog phone	
connect	44
analog trunk	
connecting	46
announcement software	132
announcements, gateway	132
ANSI/EIA/TIA-607	38
approved grounds	36
ANSI/EIA/TIA-607	38
NFPA 70: NEC	36
ASB button	116
attaching	
amphenol cable	48
Avaya Partner Contact Closure Adjunct	51
ground wires	40
Attaching	
Coupled Bonding Conductor (CBC)	50
attaching ground wires	
without ground blocks	40
AUDIX	
Avaya Aura Communication Manager	132
authentication	15
authentication file	15 , 16
Avaya Aura Communication Manager	
version requirements for SRS	15
Avaya Aura Communication Manager Messaging	132
Avaya courses	144
Avaya Gateway Manager, upgrading Java applet via	
SCP/FTP/TFTP	79
Avaya Partner Contact Closure Adjunct	51
Avaya support website	145

B

backing up the gateway	97
Backing up the gateway to USB mass storage device	97

backing up to	97
backup and restore	103
backup and restore for G430 gateway replacement	101
backup and restore operation	98
before installation	
environmental verification	16
grounding requirements	17
power outlet verification	17
site requirements	16
best practices for backup	97
box inventory	25
brackets	
attaching	26
with cable guides	27
without cable guides	27
Branch Gateway	
backing up to USB mass storage device	97
call center, announcements	132
connecting a phone	43
connecting devices	
data and voice devices	42
documentation	142
external devices	
connecting	42
installation	28 – 30
placing on a table	28
replicating to USB mass storage device	97
trunk	61
USB mass storage device	97
branch gateway backing up	98
branch gateway backup and restore	97
Branch Gateway installation	
ground conductors	35
order of installation	26
buttons	
ASB	116
RST	116

C

Call center	132
gateway announcements	132
CBC (Coupled Bonding Conductor)	50
CCA port	116
Chassis	
front panel description	113
Hardware versions	113
checking	
available number of power outlets	17
Communication Manager	84
grounding	17
hardware	83
hardware vintage	83

checking hardware vintage	83	Configuration (<i>continued</i>)	
checklist	106	telephone software, ...	60
circuit protection		trunk	61
installation	49	trunk software, ...	62
CLI		WAN	62
commands for upgrading firmware	79 , 86 , 89	configuration file	
commands for upgrading firmware, via a USB device	86	upgrade	88
troubleshooting	109	configuration files	90
upgrading firmware via SCP/FTP/TFTP	78	downloading	90
collection		configuring on	60 , 61
delete	143	connecting	
edit name	143	analog phone	44
generating PDF	143	Avaya Partner Contact Closure Adjunct	51
sharing content	143	data and voice devices	42
comcode numbers	17	DCP phones	45
Commands		external devices	42
Commands		IP phone	43
copyedge scp module	79	ISDN BRI station to ISDN port	43
copy ftp module	79	network data port	42
copy ftp phone-image	90	safety ground	39
copy ftp phone-script	90	switch port	42
copy ftp SW_imageB	79	two BRI stations	43
copy https module	79	Connecting	
copy running-config startup-config	90	Coupled Bonding Conductor (CBC)	50
copy scp module	79	telephone	60
copy scp phone-script	90	connecting to a power source	41
copy scp SW_imageB	79	Connections	
copy tftp module	79	adjunct power	130 , 131
copy tftp phone-image	90	end-to-end	131
copy tftp phone-script	90	typical adjunct power connections end-to-end	131
copy usb module	86	connectivity	56
copy usb phone-image	90	Connectivity	
copy usb phone-script	90	testing after installation	56
copy usb SW_imageA	86	considerations	96
copy usb SW_imageB	86	Console (CON) port	115
copyedge scp SW_imageB	79	contact closure	
erase phone-image	90	installing	51
ip tftp-server file-system size	90	Contact closure	
reset	90	implementing	116
show application-memory	90	port description	116
Communication Manager		content	
authentication file	15	publishing PDF output	143
license file	15	searching	143
Communication Manager web interface	84	sharing	143
Compact flash		sort by last updated	143
port	115	watching for updates	143
compact flash memory card		contents of Branch Gateway package	25
hot insertion	72	copy ftp phone-image CLI command	90
inserting	72	copy ftp phone-script CLI command	90
replacing	74	copy running-config startup-config CLI command	90
swapping	74	copy scp phone-script CLI command	90
Compact flash memory card		copy tftp phone-image CLI command	90
removing	74	copy tftp phone-script CLI command	90
configuration		copy usb module CLI command	86
gateway	53	copy usb phone-image CLI command	90
Configuration		copy usb phone-script CLI command	90
telephone	60	copy usb SW_imageB CLI command	86

Coupled Bonding Conductor	
installing	50
see CBC	50

D

description	126
Device Manager, upgrading Java applet via a USB device	86
Devices	
new, replacing and adding	59
document changes	12
documentation	
Branch Gateway	142
documentation center	143
finding content	143
navigation	143
documentation portal	143
finding content	143
navigation	143
downgrade	
compact flash to internal flash	75
downloading	90
Communication Manager	15
firmware updates	15
to local file server	81
Downloading	
IP telephone	90
downloading files	
to local file server	81
downloading to laptop	15

E

E1/T1 trunk	
connecting	47
EM200	
connecting to a power source	40
installation	30
package inventory	25
specifications	128
Emergency Transfer	
see ETR	121
Enabling	
modem	52
Endpoint devices	
new, replacing and adding	59
equipment	
unpacking	24
Equipment	
required for installation	58
erase phone-image CLI command	90
ETH LAN port	
description	116
ETH WAN	116
ETR	116 , 121
ETR port	116
example	

example (<i>continued</i>)	
using a USB device	86
using SCP/FTP/TFTP	80
example of upgrading firmware	86
example using SCP/FTP/TFTP	80
examples of	
4602SW and 4602D	92
external devices	
connecting	42
F	
Field replaceable units	
adding and removing	64
VoIP module	64
file names	
firmware	82
software	82
file server	
downloading gateway firmware to local	81
finding content on documentation center	143
finding port matrix	143
fips and non-fips mode gateways	98
FIPS mode gateway	106
firmware	17
downloading updates	15
upgrading	77 , 81 , 86
upgrading gateway	78
Firmware	
gateway	89
loading	117
upgrading	
via SCP	89
firmware file	
upgrade	88
firmware specifications	17
firmware versions	17
for fips mode gateways	103
for G430 gateway replacement	103
front panel	
gateway	116
Front panel	
Branch Gateway	113
Console (CON)	115
gateway	114 – 116
media module LEDs	126
media modules	117 – 126
ports	115 , 116
Services	115
Front panel gateway	
overview	113
system LEDs	114
Front panel gateway ports	
USB	115
Front panel media volumes	117

G

G430 cover	
removing	65
replacing	69
gateway	
firmware upgrade	79
firmware upgrades	78
Gateway	
call center	132
configuration	53
ETR	116
firmware	86
front panel	115 , 116
installation	13 , 26
ports	115 , 116
restoring from USB mass storage device	97
serial number	14
Services	115
telephone	59 , 60
trunk	61
USB mass storage device	97
voice modules, adding to	59
gateway checks	107
gateway firmware	
downloading files	86
gateway installation	
information checklist	133
restricted access location	36
gateway replacement checklist	104
ground block	
for multiple gateways	35
ground conductors	
attaching	39
location	35
grounding	
approved grounds	36
requirements	34
supplementary ground conductor	35
grounding requirements	34
grounding wires	
attaching	39

H

hardware	
vintage	83 , 84
Hot-swapping media modules	59

I

ICC- VLAN	
configuring using CLI	134
installation	
Avaya Partner Contact Closure Adjunct	51
CBC	50
contact closure	51

installation (<i>continued</i>)	
precautions	33
Installation	
equipment	58
testing	56 , 57
worksheets, preparing	80
installation checklist	133
installation hardware	13
Installation script	53
Installation site	
information	136
installing	
checklist	133
EM200	30
media modules	34
S8300 media module	33
intalling	
circuit protection devices	49
inventory of packed items	25
IP Phonephone connections	42
IP phones	
supported by local TFTP server	88
upgrading	92 , 94
IP telephones	
TFTP server upgrade example	92
upgrade files	90
upgrading	90 , 95 , 96
ip tftp-server file-system size CLI command	90
ISDN BRI station	
connect to ISDN port	43

L

LAN	
switch	42
LEDs	
media modules	118–121 , 124–126
legal notice	
license file	15
for Communication Manager	15
required for SRS	15
Lightning exposure	50
limitations	
media module combinations	31
line, configuring on	62
login	
username, passwords	134
LSP failover	
testing	57

M

media gateway installation	
information checklist	133
media module slots	114
media modules	
combination limitations	31

media modules (<i>continued</i>)	
installation	33, 34
installing	30
permitted slots	31
slot allocation	31
Media modules	
firmware	79, 86
firmware, upgrading via USB device	86
hot-swapping	59
MM710B	117
MM711	118
MM712	119
MM714	120
MM714B	120
MM716	121
MM717	123
MM720	125
MM722	126
new, replacing and adding	59
voice modules, adding	59
Messaging	
Avaya Aura Communication Manager	132
MM710	
analog trunk port	47
ISDN port	47
media module, description	117
MM710B	117
media module	117, 118
MM711	
analog DID	46
analog port	46
media module	118, 119
MM716	
analog DID port	46
MM712	
DCP ports	45
media module	119
MM714	
analog DID port	46
analog trunk port	46
media module	120
MM714B	
media module	120, 121
MM716	
attaching amphenol cable	48
connecting phones	48
media module	121–123
MM717	
attaching amphenol cable	48
connecting	
phones to MM716 and MM717	48
connecting phones	48
DCP ports	45
media module	123, 124
MM720	
media module	43, 125
ports	125
MM721	
front panel	125
media module	43
ports	125
MM722	
media module	126
overview	126
Modem	
dial backup	52
permanent connection for reporting alarms	52
USB	129
mounting	
Branch Gateway	28, 29
equipment	13
Gateway chassis	26
mounting bracket	
front	27
middle	27
mounting brackets for rack	
attaching	26
with cable guides	27
Mutual inductance coupling	50
My Docs	143
N	
NFPA 70: NEC	36
non-fips mode gateway	104
non-fips mode gateways backup and restore	101
NVRAM	
initializing with a jumper	109
O	
Obtain	
serial number	14
on gateway	61
ordering	
analog trunk	61
Ordering	
trunk	61
WAN line	62
out-of-building installation	49
over-voltage protection	49
overview	56
P	
package inventory	25
phone	
connecting to gateway	43
Physical description of Branch Gateway front panel	113
physical dimensions	127
planning	13
PLDS	
downloading software	14

port matrix	143	replacing (<i>continued</i>)	
ports	115	compact flash	74
MM720	125	Replacing	
network data port	42	endpoint devices	59
router	116	replicating the gateway	97
switch port	42	Replicating the gateway to USB mass storage device	97
Ports		replicating to	97
CCA	116	Reset button	116
CON	115	reset CLI command	90
contact closure	116	restoring backup operation	99
ETH LAN	116	restoring from	97
ETR	116	restoring the gateway	97
MM710B	117	Restoring the gateway from USB mass storage device	97
MM711	118	restricted access location	36
MM712	119	RJ-45 splitter	
MM714	120	for two BRI stations	43
MM714B	121	roadmap	
MM716	122	post installation	56
MM717	123	RST button	116
MM722	126		
Services	115	S	
switch	116	S8300	
USB	115	Server	
positioning		call center solution	132
Branch Gateway in rack	28	software upgrade	16
Post restoration useful commands	107	safety grounds	39
post-installation		SCP, FTP, TFTP or HTTPS server	
verification	56	overview	81
Power		setting up	81
connection		searching for content	143
adjunct	130	Server Values worksheets, preparing	80
cords	128	Services	
Power supplies		port	115
Adjunct systems	130	sharing content	143
pre-configuration	13	show application-memory CLI command	90
Preparation		site	
installation worksheets	80	conditions	16
Server Values worksheets	80	requirements	16
telephone configuration	60	sneak-current protection	49
trunk configuration	61	software	
WAN line configuration	62	configuration	53
Preparing		Software	
firmware installation worksheets	80	configuration	60 , 62
preparing for configuration	62	Solution Deployment Manager	78
Preserving SNMP engine ID	100	sort documents by last updated	143
Primary Management Interface (PMI)		specifications	
configuring using CLI	134	EM200	128
R		Specifications, technical	
RAM card		power cord	128
replacing	71	SRS	
upgrading	70	Avaya Aura Communication Manager version	
Remote		requirements	15
access, enabling	52	license file requirements	15
Removing installation equipment	58	supplementary ground conductor	35 , 40
replacing		support	145
		supported modem	

supported modem (<i>continued</i>)	
USB	129
supported USB modems	129
swapping compact flash	74
Switch	
port	116
system LEDs	114

T

technical specifications	127
Technical specifications	
power cord	128
Telephone	
adding to gateway	59
configuring	60
connecting	60
software configuration	60
testing	56 , 60
troubleshooting	108
telephones	56
Testing	
installation	56 , 57
telephone	60
trunk	62
WAN link	63
TFTP server	
IP phones	88
IP telephones	92
upgrading IP phones	88
TLS gateway	99
to Branch Gateway	61
training	144
troubleshooting	95
Troubleshooting	
CLI not accessible	109
gateway has no power	108
IP telephone upgrades	95
overview	108
telephone	108
trunk	
analog	61
Trunk	
adding	61
configuring	61
ordering	61
software configuration	62
testing	57 , 62
trunks	57

U

ugrading	
IP phones	92
unpacking	24
upgrade example	92
Upgrade memory kit	

Upgrade memory kit (<i>continued</i>)	
replacing the RAM card	71
Upgrade memory kit installation	70
upgrading	
configuration file	88
firmware	77
firmware file	88
gateway firmware	81 , 86
IP phones	94
Upgrading	
firmware	80 , 86
firmware installation worksheets	80
gateway firmware	78 , 79
IP telephones	90 , 95 , 96
media modules and devices	59
upgrading firmware	
using CLI via SCP/FTP/TFTP	78
upgrading gateway firmware using CLI	
via USB device	85
Upgrading gateway firmware using CLI	
via USB device	85
USB	
mass storage device	86 , 97
port	115
USB mass storage device	
upgrading gateway firmware using CLI	85
USB Modem	
supported by gateway	129
supported by S8300	129

V

videos	145
VoIP module	
field replaceable	64
inserting	66
removing	68

W

WAN	
link	62 , 63
watch list	143
Worksheets	
installation, preparing	80