Installation and Upgrades for the Avaya Branch Gateway G450

Release 6.3.5
03-602055
Issue 1
May 2014

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. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Documentation disclaimer

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

Link disclaimer

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

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Software" means Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Units may be linked to a specific, identified Server or an Instance of the Software.

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products", or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, 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, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that 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 60950-1 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. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

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

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

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

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
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	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 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

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

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

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

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 materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

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

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. 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, 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 Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://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: Before you install

Before you install

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

Related topics:

Before going to site on page 11
Site requirements on page 16
Firmware Specifications on page 18
Branch Gateway package contents on page 19

Before going to site

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

Related topics:

Required equipment on page 11
Obtaining the Branch Gateway serial number on page 12
RFA access on page 13
License file with Survivable Remote Server on page 13
Downloading license and authentication files on page 13
ART for the RAS IP address on page 14
Downloading recent firmware on page 16
The EPW on page 16

Required equipment

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

Related topics:

Equipment required for installation on page 12

Equipment required for mounting on page 12
Equipment required for installing an S8300 Server on page 12
Equipment required if you are not installing an S8300 Server on page 12

Equipment required for installation

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

Equipment required for mounting

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

Equipment required for installing an S8300 Server

- One USB CD-ROM drive
- A laptop computer with Internet Explorer

Equipment required if you are not installing an S8300 Server

- A PC on the local network, optionally with a USB flash drive
- A laptop computer running Windows XP or Windows 2000 with a serial port recognized by the operating system on the laptop. If the port is recognized, it is listed by the Device Manager.
- A modem to connect to the Branch Gateway to enable dial-in configuration. Use a serial modem (Multitech MultiModemZBA MT5634ZBA-V-V92) or a USB modem (see USB modems supported by the Branch Gateway on page 164 for a list of the USB modems supported by the Branch Gateway).USB modems supported by the Branch Gateway on page 164

Obtaining the Branch Gateway serial number

About this task

Look for the serial number sticker on the back of the Branch Gateway chassis. If the unit is delivered directly to the customer and you will not have phone or LAN line access from the

customer site to access the http://rfa.avaya.com website, this task will require a preliminary trip to the customer site.

RFA access

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

As a first-time user:

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

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

License file with Survivable Remote Server

If you are installing an S8300 as a Survivable Remote Server (SRS), the license file for the S8300 must have a Communication Manager release that is equal to or greater than that of the server that acts as primary controller (an S8300, S8400, S87xx, or S85xx). This is necessary so that if control passes to the SRS, it can allow the same level of call processing as that of the primary controller.

Additionally, the SRS must have a version of Avaya Aura® Communication Manager that is identical to that of the primary controller.

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

Downloading license and authentication files

About this task

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

Important:

If you are replacing the installed firmware with version 5.2.1, you must download a 5.2.1 authentication file before replacing the firmware.

Procedure

1. Use Windows File Explorer or another file management program to create a directory on your laptop for storing license and authentication files (for example, C:\licenses).
2. Access the Internet from your laptop and go to http://rfa.avaya.com.
3. Login using your SSO login and password.

   The AFS and RFA information home page appears.
4. Start the RFA application from the RFA information page.

   To create and download the license file and authentication file, follow the instructions outlined in the *Avaya Remote Feature Activation (RFA) User Guide*, 03-300149.
5. Use the download or email capabilities of the RFA website to download the license and authentication files to your laptop.

Result

You can use the Maintenance Web Interface to install the Communication Manager license and authentication files.

ART for the RAS IP address

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

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

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

Note:

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

Related topics:

Obtaining the RAS IP address and password on page 15

Obtaining the RAS IP address and password

Procedure

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

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

   The Start of Installation script & IP Addr Admin screen appears.
5. In the FL Number field, enter the customer's FL number.
6. In the Session Type field, select **Installation Script Administration**.
7. In the Product Type field, select **Gxxx MEDIA GATEWAY** if you want to configure remote access for the Branch Gateway, or **S8300 SERVER** if you want to configure remote access for the S8300.
8. In the INADS field, enter the number of the telephone line to which you will connect the modem.
9. Click **Start Installation script & IP Addr Admin**.

   ART validates your input and the Customer Validation screen appears.
10. Read the customer information displayed, to check that it is correct.
11. In the Customer Type field, select **Other**.
12. Click **Continue Installation Script Administration**.

    A product list appears.
13. Click the number of the product for which you are configuring remote access.

    The Gxxx MEDIA GATEWAY Installation Script Administration Data screen appears.
14. In the Product Name field, enter the product name.

15. In the INADS Number field, make sure the correct customer provided dial-in number for the Branch Gateway appears.
16. Click **Continue Installation Script Administration**.

    ART generates the RAS IP address and password (CHAP secret key) and generates an installation script for the product. Keep the RAS IP address and password to configure your modem later.
17. Click **Download Installation Script File** to download the installation script to your laptop, or **Email Installation Script File** to have the script emailed to you.

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

Downloading recent firmware

About this task

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

The EPW

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

Note:

For information on the EPW and the Avaya Installation Wizard, see the documentation for Media Gateways release 5.2.

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

Site requirements

Inspect the site before you begin the installation. Verify that the site requirements have been met for adequate environmental conditions, power and grounding availability, safety, and security conditions. If you find discrepancies between the specifications necessary for proper

installation of equipment and the conditions on site, contact your project manager before proceeding with the installation.

The Branch Gateway may be installed in a 19" rack, mounted on a wall, or placed on a sturdy table. Installation instructions are provided in Installing the Branch Gateway on page 23. The ambient temperature should be in the range 32 to 104˚F (0 to 40˚C). The humidity should not be higher than 90%.

Related topics:

Verifying temperatures and clearances on page 17
Verifying power outlets on page 17
Verifying the grounds on page 17

Verifying temperatures and clearances

About this task

Verify that temperatures and clearances are within the recommended technical parameters. Consult the table of Technical Specifications in Technical specifications on page 163.

Warning:

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

Verifying power outlets

About this task

Check that an adequate number of power outlets are available. Verify that the Branch Gateway and the other equipment in the rack do not present a possible overcurrent or overload to the customer's branch circuit and/or power distribution strip. Power requirements are listed in Power cord specifications on page 164.

Warning:

Do not overload the power circuit.

Verifying the grounds

About this task

Ensure that the installation site has access to approved grounds and that either a trained technician or a licensed electrician will be verifying all grounds and installing the Supplementary Ground Conductor (consult Attaching ground conductors on page 36).

Warning:

Installation in a Restricted Access Location and secure access are required in Finland, Norway, and Sweden. The Branch Gateway relies on two ground connections: first, the mains plugs for the power supplies are required to be connected to AC outlets that have earth contacts; and second, the Supplementary Ground Conductor provided with the system provides a non-removable ground even when the AC cords are disconnected. However, because of unreliable earthing concerns in Finland, Norway, and Sweden, the Branch Gateway must be installed in a Restricted Access Location (RAL). An RAL is defined as an access that can be gained only by trained service personnel or customers who have been instructed about the reasons for the restricted access and any safety precautions that must be taken. In these cases, access to the Branch Gateway is gained by the use of a tool (such as a lock and key) or other means of security. If you have any questions about the safety conditions, contact your project manager. When you have verified that the site is ready for a safe installation, proceed with the installation.

Firmware Specifications

New Comcode numbers for G450

- 700506953 : G450 MAIN SUPERVISOR BOARD V3
- 700506954 : G450 MAIN SUPERVISOR BOARD V3 NON GSA
- 700506955 : G450 MP160 MEDIA GATEWAY
- •700506956 : G450 MP160 MEDIA GATEWAY NON GSA
- 700506959 : G450 MP80 WITH V3 SVP BOARD
- 700506960 : G450 MP80 WITH V3 SVP BOARD
- 700508199 : G450 160 CHANNEL DSP daughter board

Minimum firmware requirements for G450

		v1a	v2b	v2d	v3b	Recommended CM Version
BGW 5.0	27.31.0	Yes	Yes	Yes	No - require new FW (base not supported)	CM 5.0 (SP)
BGW 5.1	28.27.0	Yes	Yes	Yes	No - require new FW (base not supported)	CM 5.1 (SP)
BGW 5.2	29.24.0	Yes	Yes	Yes	No - require new FW (base not supported)	CM5.2 (SP)

		v1a	v2b	v2d	v3b	Recommended CM Version
BGW 5.2.1	30.28.0 +	Yes	Yes	Yes	Yes (min FW load 30.28.0)	CM 5.2.1 (SP 16) or higher AA 6.3 FP3 CM6.3 .2 +
BGW 6.1	31.26.0	Yes	Yes	Yes	No - require new FW (base not supported)	CM 6.0.1 - Nov 2010
BGW 6.2.1	32.26.0	Yes	Yes	Yes	No - require new FW (base not supported)	AA 6.2 FP1-CM 6.2 sp4 - Dec 2012
BGW 6.3	33.13.0	Yes	Yes	Yes	No - require new FW (base not supported)	AA 6.2 FP2-CM 6.3 - May 2013
BGW 6.1 JITC	33.13.1	Yes	Yes	Yes	Would require JITC request	CM 6.3.1.1 (JITC SP)
BGW 6.3.1	34.6.0 +	Yes	Yes	Yes	Yes (min FW load 34.6.0)	AA 6.2 FP3 CM 6.3.2 + (Oct 2013) AA 6.2 FP 2 CM 6.3 & CM 5.2.1 SP 16+
BGW 6.3.5	35.x.y	Yes	Yes	Yes	Yes	AA 6.2 FP3 CM 6.3.2 + AA 6.2 FP 2 CM 6.3 & CM 5.2.1 SP 16+
BGW 6.3.6 JITC	36.x.y	Yes	Yes	Yes	Yes	AA 6.2 FP 4 CM 6.3.6 AA 6.2 FP3 CM 6.3.2 &CM 5.2.1 SP 16+

Branch Gateway package contents

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

- One Branch Gateway chassis. The required media modules may be installed.
- One accessories box, containing:
  - Two 19” mounting brackets
  - One cable management assembly

- One Supplementary Ground Conductor
- Fifteen 3/8" flat head screws
- One 5/16" crosspoint screw for grounding
- One washer for grounding
- One ground screw
- Four rubber feet
- One jumper for bridging NVRAM init pins

• Auto-run CD

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

Related topics:

Removing power supply units on page 20
Unpacking and checking package contents on page 20

Removing power supply units

About this task

For ease of installation and to enable single-person installation, it is recommended to remove the power supply unit(s) before unpacking the Branch Gateway.

Procedure

1. Open the package.
2. Turn the Branch Gateway, so that the rear panel is facing up.
3. Remove the power supply unit (PSU).
   If you ordered two PSUs, remove them both.
   a. Loosen the two PSU captive screws, one on each side of the PSU.
   b. Grasp the two side handles and pull the PSU up and out.
   c. Place the PSU carefully on the table.

Unpacking and checking package contents

About this task

For the Branch Gateway package:

Procedure

1. Unpack the Branch Gateway and accessories.

Electrostatic alert:

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

2. Check the contents of the packaging against the customer order.
3. Cross-check the customer order with the planning documentation you have been given.

   Media modules, telephones and other equipment are listed on your planning and shipping documentation. Placement for the media modules and other equipment are also indicated.
4. Verify that all necessary elements have been received and are in good condition.

   If there are missing or damaged elements, contact your project manager. The planning documentation will list contact information for key personnel.

Result

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

Chapter 2: Installing the Branch Gateway

Branch Gateway installations

Installing the Branch Gateway consists of installing the Branch Gateway chassis, power supply, and media modules, attaching ground conductors, and connecting the power.

Related topics:

Roadmap for installing the Branch Gateway on page 23
Mounting the Branch Gateway chassis on page 24
Installing the Power Supply Units on page 30
Installing the media modules on page 30
Ground conductor attachments on page 36
Connecting power to the Branch Gateway on page 44

Roadmap for installing the Branch Gateway

About this task

Install these devices in the following order using the appropriate procedure described in this section:

Procedure

1. Branch Gateway chassis
2. Power Supply Units
3. Media modules
4. Ground conductors
5. Power to the Branch Gateway

Mounting the Branch Gateway chassis

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

Electrostatic alert:

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

Note:

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

Related topics:

Branch Gateway racks on page 24
Mounting the Branch Gateway on a wall on page 28
Placing the Branch Gateway on a table on page 29

Branch Gateway racks

The Branch Gateway mounts in a standard 19-inch rack.

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

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

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

Related topics:

Brackets without cable guides on page 25
Attaching a mounting bracket to the front of the Branch Gateway on page 25
Attaching a mounting bracket to the middle of the Branch Gateway on page 25
Brackets with cable guides on page 25
Attaching a mounting bracket with cable guides on page 26
Attaching each mounting bracket to the Branch Gateway on page 26

Before mounting the Branch Gateway on page 27
Mounting the Branch Gateway in the rack on page 27

Brackets without cable guides

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

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

Attaching a mounting bracket to the front of the Branch Gateway

About this task

Attaching a mounting bracket to the middle of the Branch Gateway

About this task

Brackets with cable guides

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

Note:

It is recommended to attach the mounting bracket with cable guides to the left side of the rack, so that the cables will not interfere in the event that you replace the fan tray. However,

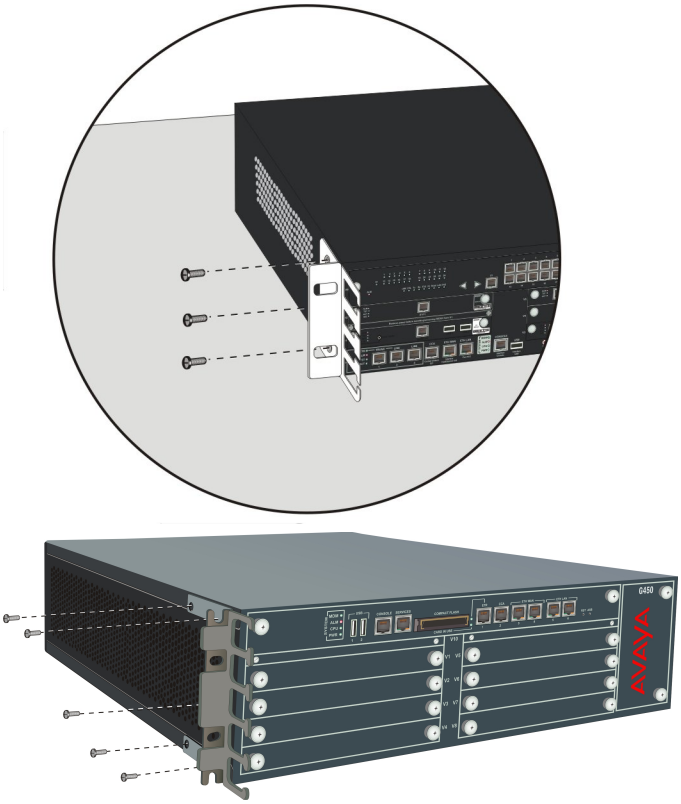
iIf you are installing an MM717 or MM716 media module, attach the mounting bracket with cable guides to the right side of the rack, to support the weight of the amphenol cable you will connect to the MM717 or MM716 media module. See Connecting a DCP telephone to an MM712 or MM717 media module on page 50.

Note:

Connecting a DCP telephone to an MM712 or MM717 media module on page 50

Attaching a mounting bracket with cable guides

About this task



Attaching each mounting bracket to the Branch Gateway

About this task

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

Procedure

1. Position a bracket over the desired mounting position.

2. Affix the bracket to the chassis with five of the fifteen 6-32 x 3/8 screws provided.
3. Tighten with a screwdriver.

Before mounting the Branch Gateway

Procedure

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

Result

Note:

The Branch Gateway weighs 21 pounds (9.5 kg) completely empty and up to 44 pounds (20 kg) when equipped with media modules, an S8300 Server, and two power supply units.

Note:

Mounting the Branch Gateway in the rack

About this task

The Branch Gateway is designed for single-person mounting. This assumes that the power supplies were removed (see Removing power supply units on page 20).

Procedure

1. Insert two mounting screws, one on either side of the rack.
   These will be the bottom screws of the mounting brackets. Turn the screws only 3-4 times, so that a part of them is protruding.
2. Position the Branch Gateway in the rack so that the bottoms of the brackets are resting on the protruding screws.
3. Position the Branch Gateway in the rack.
   Ensure that there is adequate ventilation.
4. Insert four rack mounting screws, two on each side.
5. Verify that the Branch Gateway is level and horizontal.
6. Tighten the rack mounting screws.
   Avoid overtightening.

7. Either tighten the two bottom-most screws inserted in step 1 on page 0 , or remove them completely.
8. Verify that ventilation vents are not obstructed.

Result

At this point, you have mounted the Branch Gateway chassis in the rack and are ready to insert media modules as required in the planning documentation.

Mounting the Branch Gateway on a wall

About this task

To mount the Branch Gateway on a wall, use the two mounting brackets without cable guides. You can also add a mounting bracket with cable guides if desired, as explained in Brackets with cable guides on page 25.

Warning:

Only service-trained personnel are to wall-mount the Branch Gateway.

Caution:

One person may wall mount a G450 if the PSUs are removed. See . A minimum of two installers is required to wall-mount a Branch Gateway with the PSUs installed.

Caution:

If you are installing the Branch Gateway in the United States of America:

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

Related topics:

Attaching brackets to the Branch Gateway for wall mounting on page 28
Fastening the Branch Gateway to the wall on page 29

Attaching brackets to the Branch Gateway for wall mounting

About this task

Attach a bracket to each side of the Branch Gateway, as shown in the figure.

Figure 1: Attaching a bracket to each side of the Branch Gateway

Fastening the Branch Gateway to the wall

About this task

Note:

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

Procedure

1. If the wall does not have a portion of plywood available, mount a plywood sheet at least ¾ in (2.0 cm) thick and at least 4 x 4 ft (1.2 x 1.2 m) in size, horizontally onto the wall.

   Make sure the plywood is sufficiently anchored in the wall. Use a minimum of four wood screws and ensure the screws are driven into wall studs, or use four wall anchors rated not less than 50 pounds (22.5 kg) shear strength each.
2. Mark the plywood with the location of the Branch Gateway bracket screw holes before fastening the plywood to the wall.
3. Position the Branch Gateway so that its front panel is facing up, and secure it to the plywood using a minimum of four screws (pan head at least ¾ in, #10-12 screw).

Placing the Branch Gateway on a table

About this task

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

Procedure

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

Installing the Power Supply Units

About this task

When the Branch Gateway chassis is installed, first insert the power supply unit(s) if you removed them before installation (see Removing power supply units on page 20).

Procedure

1. Position the power supply unit before the opening at the rear of the Branch Gateway and engage both sides of the PSU in the interior guides.
2. Slide the PSU slowly into the chassis, maintaining an even pressure to assure that the PSU does not become twisted or disengaged from the guides.
3. Close and tighten the two PSU captive screws, one on each side of the PSU.

Result

Figure 2: Inserting the power supply unit

Installing the media modules

When the Branch Gateway chassis is installed and the power supply unit(s) have been inserted, you can insert the media modules. Each module is shipped with two thumb screws for securing the module in the Branch Gateway chassis.

Note:

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

Related topics:

[Before inserting media modules into the Branch Gateway chassis](#) on page 31
[Combination limitations](#) on page 31
[Slot allocations](#) on page 31
[Inserting the S8300 Server](#) on page 33
[Inserting media modules](#) on page 35

Before inserting media modules into the Branch Gateway chassis

- Do not install an unsupported combination of media modules. See [Combination limitations](#) on page 31.
- Allocate a permissible slot to each media module. See [Slot allocations](#) on page 31.

Warning:

Do not operate the Branch Gateway with any open slots. Failure to cover empty slots with the supplied blank plates can cause overheating due to inadequate air distribution.

Combination limitations

The following limitations apply to combining media modules in the Branch Gateway:

- Three MM340/MM342 WAN modules
- Up to seven MM721 modules
- The MM760 is not supported

Slot allocations

The Branch Gateway chassis has eight media module slots, marked V1, V2, V3, V4, V5, V6, V7, V8. Each media module is restricted to certain slots.

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

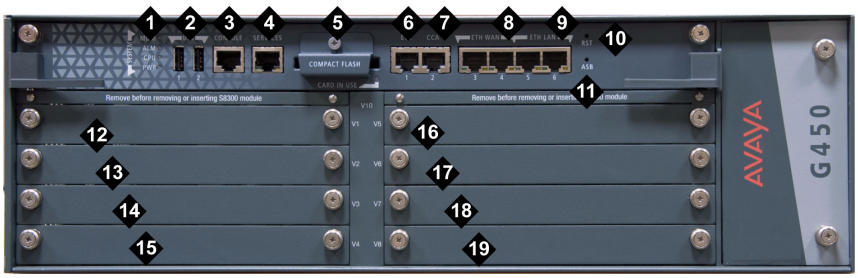


Figure 3: The Branch Gateway G450 front panel ports and slots

Table 1: Figure notes:

1. System LEDs
2. USB ports
3. Console port
4. Services port
5. Compact flash slot
6. ETR (Emergency Transfer Relay) port
7. CCA (Contact Closure) port
8. ETH WAN ports
9. ETH LAN ports
10. RST button
11. ASB button
12. V1 — slot for standard media module or S8300 Server
13. V2 — slot for standard media module
14. V3 — slot for standard media module
15. V4 — slot for standard media module
16. V5 — slot for standard media module
17. V6 — slot for standard media module
18. V7 — slot for standard media module
19. V8 — slot for standard media module

Table 2: Permitted slots for media modules

Media module	Permitted slots	Description
MM340	V3, V4, V8	Provides one E1/T1 WAN port for connecting to a WAN endpoint device.
MM342	V3, V4, V8	Provides one USP WAN port for connecting to a WAN endpoint device.

Media module	Permitted slots	Description
MM710	V1 – V8	Provides one E1/T1 trunk port for connecting an E1/T1 telephone trunk.
MM710B	V1 – V8	Provides one E1/T1 trunk port for connecting an E1/T1 telephone trunk.
MM711	V1 – V8	Provides eight universal analog ports for connecting analog telephones or trunks.
MM712	V1 – V8	Provides eight ports for connecting DCP telephones.
MM714	V1 – V8	Provides four analog ports for analog telephones and four analog ports for analog trunks.
MM714B	V1 – V8	Provides four analog ports for analog telephones, four analog ports for analog trunks, and an emergency transfer relay.
MM716	V1 – V8	Provides one amphenol connector that connects to a punch down block to provide 24 analog line ports.
MM717	V1 – V8	Provides one amphenol connector that connects to a punch down block to provide 24 ports for connecting DCP telephones.
MM720	V1 – V8	Provides eight ports for connecting up to eight ISDN trunks or 16 ISDN BRI stations.
MM722	V1 – V8	Provides two ports for connecting ISDN trunks.
S8300B/ S8300C/S8300D	V1	Server

Inserting the S8300 Server

About this task

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

Electrostatic alert:

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

Caution:

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

Caution:

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

Procedure

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

Figure 4: Inserting the S8300 Server

5. Apply firm pressure to engage the connectors.

   The connector has pins of different lengths. The long pins engage first to provide grounding. Medium length and short pins provide power and signal.
6. Lock the S8300 Server module into the chassis by tightening the spring-loaded captive screws on the front of the module.

   If you are installing an S8300, replace the plate labelled “Remove before removing or inserting S8300 module” above slot V1 and tighten the screws on the front of the plate.
7. After you have inserted the S8300 Server module, if applicable, insert the rest of the media modules.

   Make sure to insert each module in a permissible slot.

Result

Danger:

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

Inserting media modules

About this task

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

Electrostatic alert:

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

Caution:

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

Caution:

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

Procedure

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

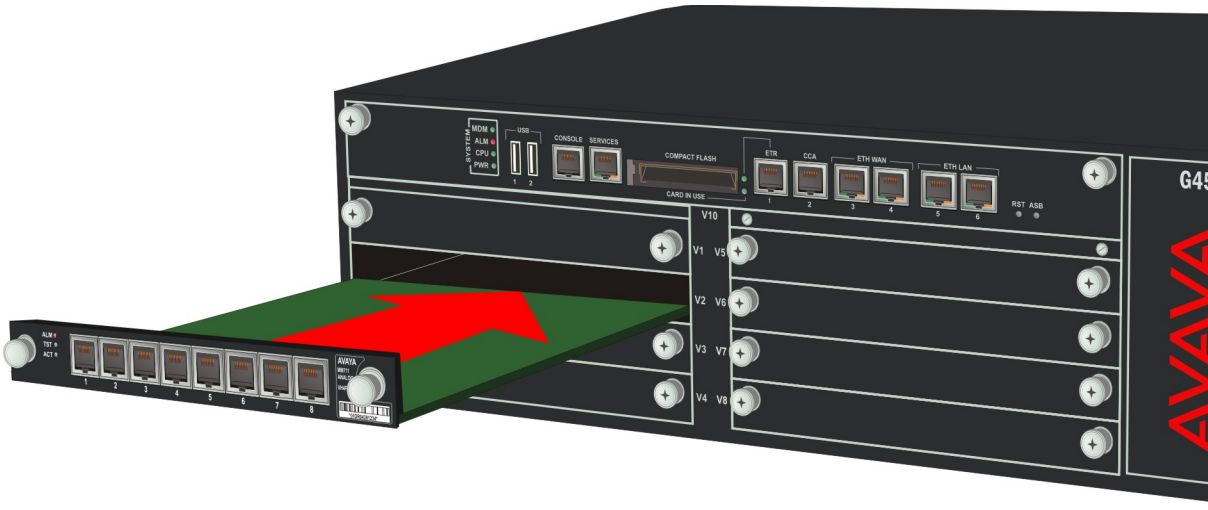


Figure 5: Inserting a media module

3. Apply firm pressure to engage the connectors.

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

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

Result

Danger:

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

Warning:

After you have connected telephones to the various media modules, be sure to add circuit protection to the lines.

Ground conductor attachments

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

Warning:

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

Related topics:

General grounding requirements on page 37
Approved grounds on page 38
Safety ground connections on page 42

General grounding requirements

Note:

Grounding requirements differ widely from country to country. In addition to the grounding instructions presented in this section, you must follow the local electrical installation codes for your location.

Two safety grounds are required to ensure safe operation of the Branch Gateway: the ground conductor that is part of the AC power cord, and the field-installed green/yellow conductor referred to as the Supplementary Ground Conductor. Both safety grounds must be connected to an approved ground. If a power cord accompanies the Branch Gateway, use that cord whenever possible.

Related topics:

Installation location on page 37
Ground conductor on page 37
Ground block on page 37
Restricted Access Location on page 38

Installation location

Select a location for the Branch Gateway installation that is close enough for use with the supplied secondary grounding conductor. If this location requirement is not met, contact a licensed electrician to install a Supplementary Ground Conductor per Article 250 of the National Electrical Code (NEC).

Warning:

If the installation location is greater than the length of the supplied secondary grounding conductor from an approved ground, do not install the Branch Gateway until a licensed electrician is present to install a Supplementary Ground Conductor.

Ground conductor

A Supplementary Ground Conductor is provided with the equipment, and is constructed of 10 AWG (4.0 mm^2) wire, with an insulated ring terminal crimped to one end that is suitable for the #8 (M4) stud/screw on the rear of the Branch Gateway chassis.

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

Ground block

A ground block, supplied by the customer and installed by an electrician, is available for use when you are installing multiple Branch Gateways . The ground block, intended for rack mounting, has ten terminals available for terminating Supplementary Ground Conductors. Up to ten Branch Gateways can be grounded at the block installed close to the equipment (on a

rack) and then a single ground conductor can be routed from the same block to an approved ground.

Danger:

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

Restricted Access Location

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

Warning:

For installations in Finland, Norway, and Sweden, the Branch Gateway 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.

The first is based on NFPA 70: National Electrical Code (NEC – a United States code).

Note:

Compliance with NFPA 70: NEC – or – with the equivalent local electrical code/grounding requirements is mandatory.

The second is based on ANSI/EIA/TIA-607 (Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications).

Note:

ANSI/EIA/TIA-607 (TIA-607) defines an intra-building ground-wiring scheme for communications equipment, and specifies equipment connection/grounding points according to that scheme. TIA-607 assumes the underlying building grounding infrastructure is in compliance with NFPA 70: NEC. Compliance with the NEC (or the equivalent local electrical code/grounding requirements) is essential for the proper application of TIA-607.

Compliance with NFPA 70: NEC will provide suitable grounding for the Avaya equipment. TIA-607 provides an enhanced, communications-specific grounding scheme: where TIA-607 has been implemented the Avaya equipment shall be grounded per this method.

Important:

- Ensure that the installation site has access to approved grounds and that either a trained technician or a licensed electrician will be verifying all grounds and installing the Supplementary Ground Conductor.
- If you have difficulty interpreting the grounding methods in this document, Avaya recommends obtaining the services of a certified power contractor or auditor prior to system installation or cutover.

Warning:

Failure to follow grounding recommendations can result is a system installation that is:

- Unsafe for personnel handling or using the equipment
- Not properly protected from lightning or power transients
- Subject to service interruptions

NFPA 70: NEC

In buildings without a ground-cabling infrastructure meeting TIA-607 the Avaya equipment shall be grounded by connection to the nearest accessible location on one of the following approved building grounds:

Note:

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 consult the 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 –

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

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 shall not rely only on the metal water pipe for grounding: a supplemental ground is required. (See NEC Article 250.53 for additional details.)

Metal Frame of the Building:

The metal frame member (I-beam, pillar) must be connected to earth by one of the following methods –

- Be in direct contact with the earth, or encased in concrete that is in direct contact with the earth, for at least 3 meters (10 feet).
- Be connected to the reinforcing bars of a concrete-encased electrode. The electrode must be encased by at least 5.1 cm (2 inches) 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 6.1 meters (20 feet) of one or more steel reinforcing bars or rods, 1.3 cm (0.5 inches) in diameter, or at least 6.1 meters (20 feet) of bare solid copper, 4 AWG ($26mm^2$) wire.
- Be connected to a ground ring. A ground ring is a buried ground that encircles a building, having a length of at least 6.1 meters (20 feet) of 2 AWG ($35mm^2$) bare copper wire.
- Be connected to rod and pipe electrodes. A rod or pipe electrode consists of one 1.6 cm (5/8 inch) solid rod or 2 cm (3/5 inch) conduit driven to a minimum depth of 2.4 meters (8 feet).
- Be connected to plate electrodes. Plate electrodes have a minimum of 0.185 square meter (2 square feet) 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 may include the following:

- Metal Frame of the Building (in accordance with the criteria specified in Metal Frame of the Building on page 40)
- 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 only be accessed inside a dedicated power equipment room, then connections to the ground must be made by a licensed electrician.

ANSI/EIA/TIA-607:

In buildings where a ground-cabling infrastructure meeting TIA-607 has been implemented the Avaya equipment shall be grounded according to the TIA-607 standard. In a TIA-607

installation, the Telecommunications Main Grounding Busbar (TMGB)/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.

Refer to Figure 6: ANSI/TIA/EIA-607 Grounding Schematic on page 41.

Configure telecommunications subsystems, such as groups of frames or equipment, as separate single-point ground entities connected to the equipment's dedicated service panel via a single-point ground bar. The service panel ground connects to the building principle ground via the main service panel or, in a TIA-607 installation, via the TGB. Refer to Figure 7: Typical Wiring Plan on page 42.

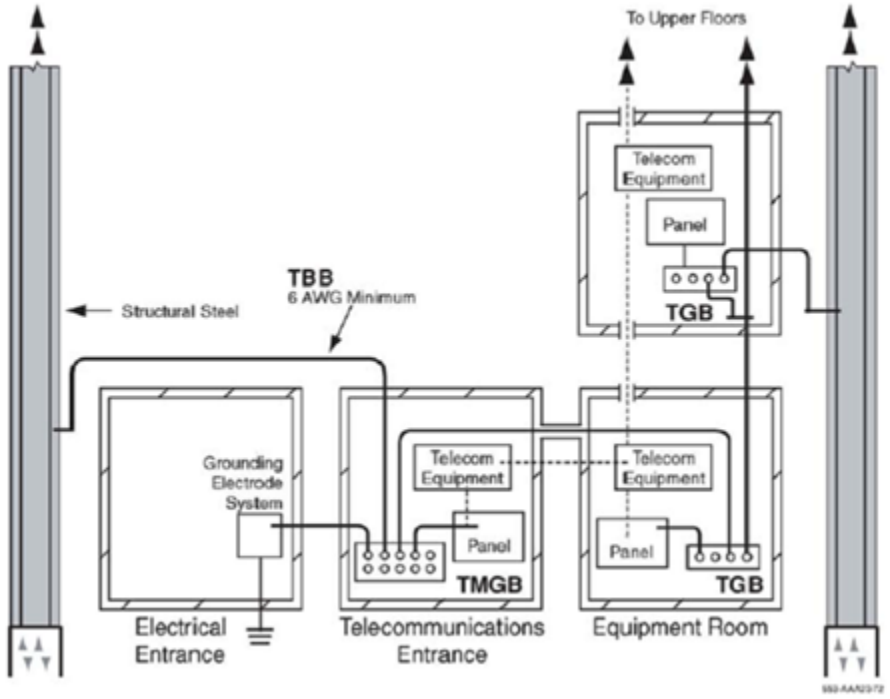


Figure 6: ANSI/TIA/EIA-607 Grounding Schematic

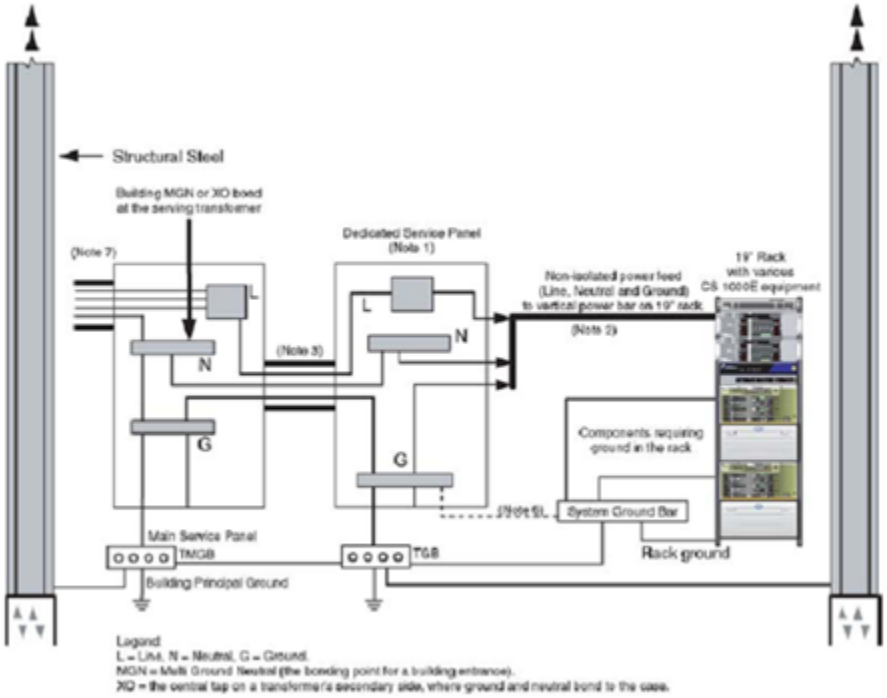


Figure 7: Typical Wiring Plan

Safety ground connections

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

Local electrical installation codes must be followed when installing the Branch Gateway.

Danger:

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

Warning:

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

Related topics:

Attaching the ground wires on page 43
PWR LED indications on page 44

Attaching the ground wires

About this task

Procedure

Place the ring terminal of the 10 AWG (4.0 mm^2) Supplementary Ground Conductor on the ground screw that was provided in the accessories box.

Related topics:

Attaching ground wires for purchased ground blocks on page 43
Attaching ground wires for unused ground blocks on page 43

Attaching ground wires for purchased ground blocks

Procedure

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

   Do not coil the Supplementary Ground Conductor.

2. Attach one end of the remaining 10 AWG (4 mm^2) ground wire to one of the terminals in the ground block and the other end to an approved ground.
3. Cut this ground wire to the length needed to reach the approved ground.

   Do not coil this wire.

Result

Note:

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

Attaching ground wires for unused 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 chassis.
3. If you have a second power supply unit, you can connect it to power by repeating steps 1 on page 44 and 2 on page 44.

Result

Note:

If two PSUs are installed in the Branch Gateway, the PWR LED blinks if only one PSU is connected to power, and stays on if both PSUs are connected to power.

PWR LED indications

The PWR LED on the power supply unit indicates the operational status of the power supply unit.

Table 3: Power Supply Unit PWR LED

LED	Name	State	Color	Indication
PWR	Power	On	Green	Power is OK
		On	Red	A power fault
		Off		The PSU unit is broken or not powered

Connecting power to the Branch Gateway

About this task

After you have mounted the Branch Gateway, installed the PSU(s), installed the media modules, and attached grounding conductors, you can connect power to the Branch Gateway. The Branch Gateway can be ordered with either one or two power supply units.

Procedure

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

   The Branch Gateway is now powered.

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

Chapter 3: Connecting devices

Connecting devices

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

Warning:

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

Related topics:

Roadmap for connecting devices on page 45
Data and voice device connections on page 45

Roadmap for connecting devices

Connect these devices in the following order using the appropriate procedure described in this section:

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

Data and voice device connections

There are various possible ways of connecting different devices. See your planning documentation for any topology requirements to connect specific devices to specific ports. As

you connect devices, keep a record of the slots and ports into which specific devices are connected. You will need this information when configuring the Branch Gateway.

Related topics:

Switch or network data port connections on page 46
IP telephone connections on page 46
ISDN BRI station connections on page 47
Connecting an analog telephone on page 49
Connecting a DCP telephone to an MM712 or MM717 media module on page 50
Connecting an analog trunk on page 51
Connecting an analog DID trunk on page 51
Connecting an E1/T1 trunk on page 52
Connecting an ISDN BRI trunk on page 52
Connecting devices to the MM717 and MM716 media modules on page 53
Circuit protection installation on page 54
WAN connections on page 55
Coupled Bonding Conductor installations on page 57
Avaya Partner Contact Closure Adjunct installations on page 58
808A Emergency Transfer Panel and associated telephones installations on page 58

Switch or network data port connections

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

IP telephone connections

Note:

For a full list of supported phones, see Appendix B, *Supported Avaya telephones* in *Overview for the Avaya G450.*

Connect the IP telephone to an external Ethernet switch. This switch must be connected to a LAN port on the Avaya Branch Gateway G45 . This port is labeled 10/5 or 10/6.

If the telephone is not an Avaya IP telephone, you can connect it to any port on the network switch. Note the slot and port number on the Avaya Branch Gateway G450 to which you connect the telephone.

Related topics:

Connecting the telephone to the Branch Gateway on page 47

Connecting the telephone to the Branch Gateway

Procedure

1. Wire a telephone to a port on the switch connected to the Branch Gateway LAN port.

   If the switch is a PoE switch, you do not need to plug the IP telephone into a power supply.
2. Plug the telephone into the telephone port.
3. If the IP telephone is powered independently, plug the IP telephone into a power supply.

   Check that the IP telephone is powered up.

ISDN BRI station connections

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

Note:

The MM720 and MM721 BRI media modules cannot be administered to support both BRI trunks and BRI stations at the same time. However, the MM720 and MM721 BRI media modules support combining both B-channels together to form a 128-kbps channel. Communication Manager 3.1 enables combining B-channels, using BONDing, to form a higher bandwidth connection. Finally, if the MM720 or MM721 BRI media module is administered to support BRI stations, it cannot be used as a clock synchronization source.

Related topics:

Connecting one ISDN BRI station to one ISDN port on page 47
Connecting two ISDN BRI stations to one ISDN port on page 47

Connecting one ISDN BRI station to one ISDN port

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

Connecting two ISDN BRI stations to one ISDN port

Procedure

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

   See the figure on page 48 for the correct wiring for the splitter.

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

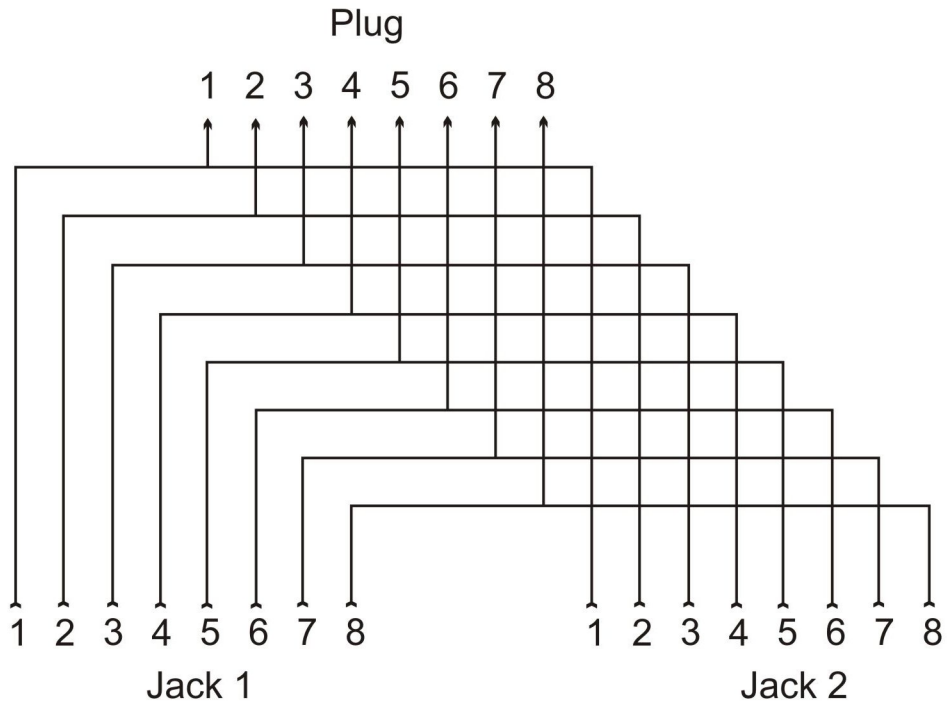


Figure 8: RJ-45 splitter wiring for connecting two ISDN BRI stations to one ISDN port

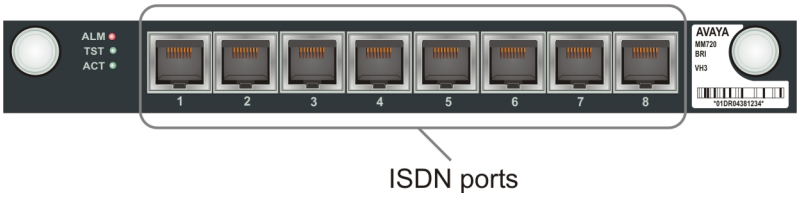


Figure 9: The MM720 media module

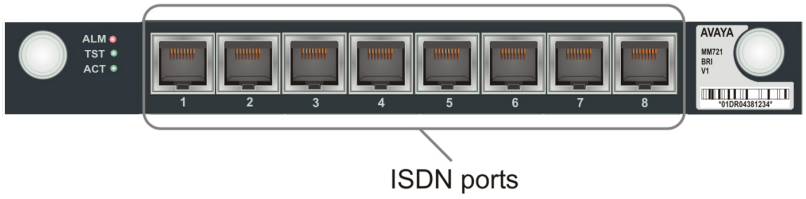


Figure 10: The MM721 media module

Connecting an analog telephone

About this task

Note:

For a full list of supported phones, see Appendix B, *Supported Avaya telephones* in *Overview for the Avaya Branch Gateway G450.*

Procedure

1. Wire a telephone port to one of the following analog ports:
   - A universal analog port on an MM711 media module
   - Any analog line port on a punch down block connected to an MM716 media module. To connect the MM716 media module to a punch down block to enable telephone connection, see Connecting devices to the MM717 and MM716 media modules on page 53.
   - A LINE port on an MM714 or MM714B media module
2. Plug the analog telephone into the telephone port.

Result

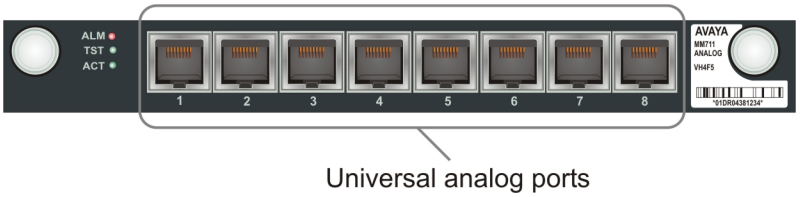


Figure 11: The MM711 media module

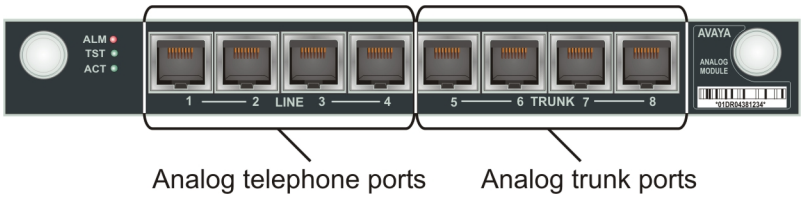


Figure 12: The MM714 media module

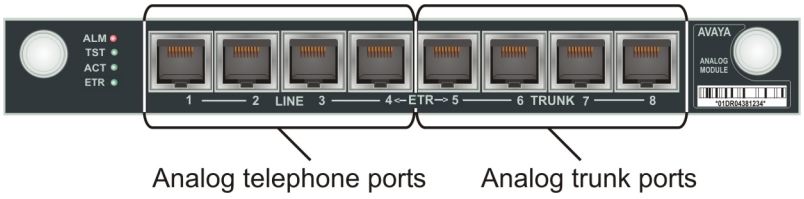


Figure 13: The MM714B media module

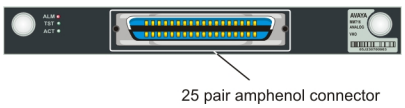


Figure 14: The MM716 media module

Note:

Analog line ports support the following maximum distances:

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

Connecting a DCP telephone to an MM712 or MM717 media module

About this task

Note:

For a full list of supported phones, see Appendix B, *Supported Avaya telephones* in *Overview for the Avaya Branch Gateway G450.*.

Warning:

Avaya MM712 and MM717 DCP Lines. DCP lines require the 146E IROB (In-range, Out of Building) protectors, or the 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 the Branch Gateway.

The following media modules provide DCP telephone ports:

- MM712. Eight DCP ports
- MM717. Twenty four DCP ports, provided via a single 25-pair amphenol socket on the front panel. To connect the MM717 media module to a punch down block to enable telephone connection, see Connecting devices to the MM717 and MM716 media modules on page 53.

Figure 15: The MM312 media module

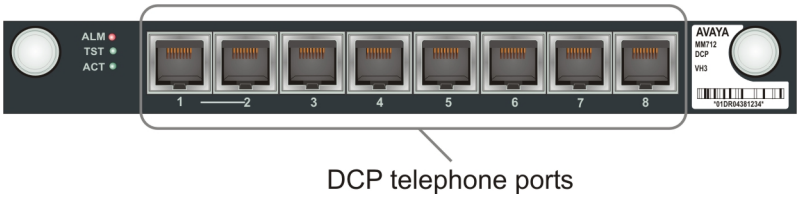


Figure 16: .The MM712 media module

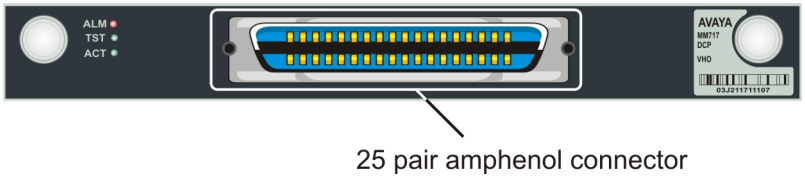


Figure 17: .The MM717 media module

Connecting an analog trunk

Procedure

Connect the trunk to one of the following ports:

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

Connecting an analog DID trunk

Procedure

Connect the trunk to one of the following ports

- Any universal analog port on an MM711 media module
- Any analog line port on a punch down block connected to an MM716 media module.

  To connect the MM716 media module to a punch down block to enable trunk connection, Connecting devices to the MM717 and MM716 media modules on page 53.
- One of the ports marked Line on an MM714 or MM714B media module
- The TRUNK port on the Branch Gateway front panel.

Note:

The TRUNK analog telephone port on the Branch Gateway front panel forms a mechanical analog relay with the LINE port next to it. This relay can be configured 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 telephone plugged into the LINE port. Conversely, the telephone plugged into the LINE port can use the trunk during an emergency situation to make outgoing calls.

Connecting an E1/T1 trunk

About this task

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

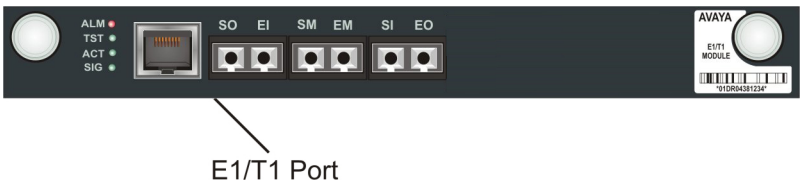


Figure 18: The MM710B media module

Connecting an ISDN BRI trunk

About this task

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

Note:

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

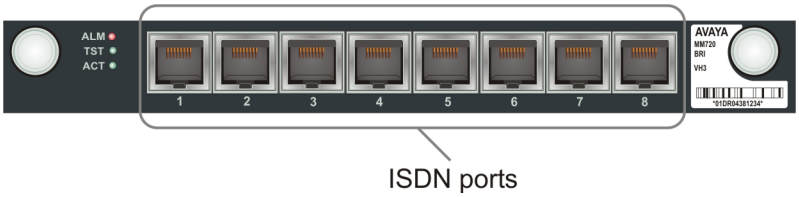


Figure 19: The MM720 media module

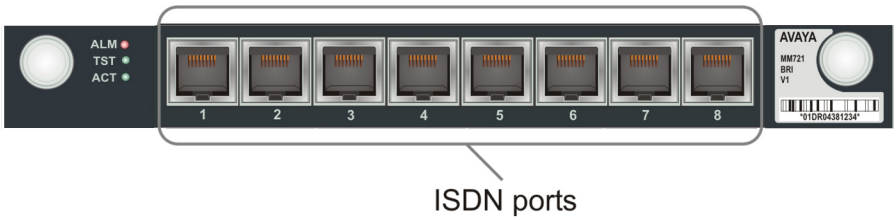


Figure 20: The MM721 media module

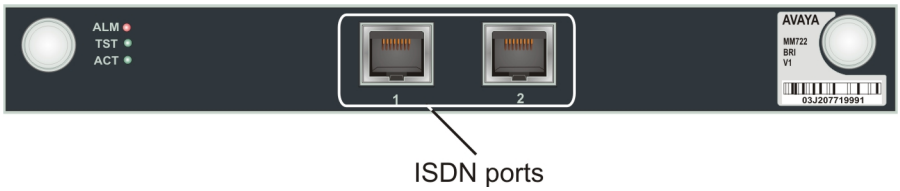


Figure 21: The MM722 media module

Connecting devices to the MM717 and MM716 media modules

About this task

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

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

  You can terminate up to 24 endpoint devices on the connected punch down block.

Related topics:

[Connecting the MM716 or MM717 front panel connector to a punch down block](#) on page 53

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

Procedure

1. Connect one end of a CAT5 cable with a 25-pair amphenol connector at each end to the 25-pair socket on the MM716 or MM717 front panel, so that the cable extends to the right of the Branch Gateway.

   The cable you use must be such that the connector you plug into the media module is 90˚ to the cable.

2. Tighten the end screw of the amphenol connector to securely fasten the connector to the left side of the front panel socket.
3. Thread a tie wrap through the small bracket to the right of the front panel socket.
4. Fasten the tie wrap around the cable to secure the cable to the right side of the front panel socket.

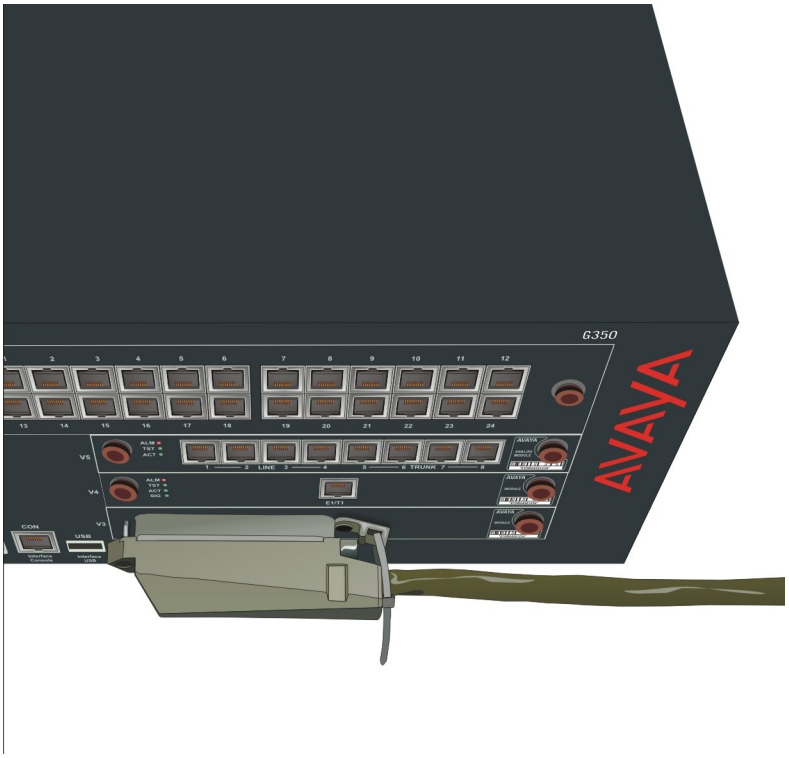


Figure 22: Attaching and securing the amphenol cable to the MM716 or MM717 25-pair socket

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

Result

You can now connect endpoint devices to the RJ-11 jacks. For the pin-out of the 25-pair connector, see the table on page 157.

Circuit protection installation

Protection from over-voltages (lightning, power line induction) and over-currents (sneak currents) is required for ALL off-premises (out-of-building) trunks, lines, and terminal installations.

Campus installations (interbuilding cabling) of telephones or other standard (tip / ring) devices require over-voltage and sneak current protection in both buildings.

Over-voltage and sneak current protectors must be Listed devices, and installed in accordance with NFPA 70: NEC Article 800 (subsections “Protective Devices” and “Cable and Primary Protector Bonding and Grounding”), or must comply with 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 protection devices have been approved for use with the G450 Gateway:

- For the Avaya MM710, MM710B T1/E1, or MM340 media modules: Over-voltage and sneak current protection for the Avaya MM710, MM710B and MM340 are provided on the media modules.
- For the Avaya MM711, MM714, MM714B, and MM716 Analog media modules: Incoming trunks normally have over-voltage protection provided by the local telephone company. Analog voice terminals use one of the following types of combined over-voltage and sneak current protection at both building entry points:
  - Gas tube with heat coil. 4B1E-W
  - Solid state with heat coil. 4C1S
  - IROB. 146C (4– also called ITW Linx MCO4X4) or 146H (25 - lines – also called ITW Linx MCO25)
- For the Avaya MM712 and MM717 DCP media modules: either the 146E IROB (2- lines – also called ITW Linx MDS2) or the ITW Linx MDS25 (25 two-wire lines) or the 4C3S-75 solid state protectors for over-voltage and sneak current.
- For the Avaya MM722 ISDN-BRI media modules: over-voltage and sneak current protection are provided on the media modules.
- For the Avaya MM720 and MM721 ISDN-BRI media modules: network-side applications require an NT-1 device. Tie trunk applications going off-premises (out-of-building) require either the 146E IROB (2- lines – also called ITW Linx MDS2) or the ITW Linx MDS25 (12 four-wire lines) IROB (In-Range Out-of-Building) or 4C3S-75 solid state protectors for over-voltage and sneak current.

Warning:

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

WAN connections

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

Related topics:

WAN to Branch Gateway connections on page 56
Connecting an Ethernet WAN link on page 57
Connecting an external router to the Branch Gateway on page 57

WAN to Branch Gateway connections

There are some differences in how to connect the WAN, depending on the type of WAN link you are connecting.

Related topics:

Connecting a WAN link to the MM342 media module on page 56
Connecting an E1/T1 WAN link to the MM340 media module on page 56

Connecting a WAN link to the MM342 media module

About this task

You must connect the WAN link to a device connected to the Avaya MM342 media module.

Procedure

To connect the WAN link, plug the WAN line into the USP port on the MM342 media module. This port is marked USP. To connect the WAN line to the port, use one of the following cable types, depending on the service provider's equipment:

- Avaya Serial Cable DTE V.35
- Avaya Serial Cable DTE X.21

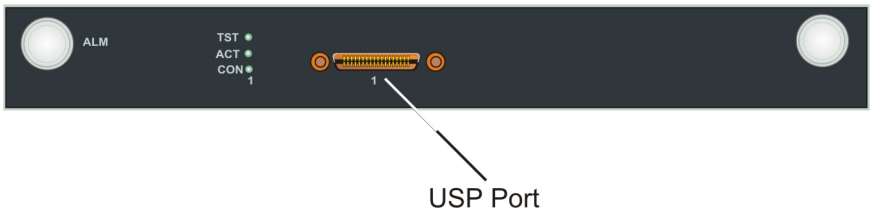


Figure 23: The MM342 media module

Connecting an E1/T1 WAN link to the MM340 media module

About this task

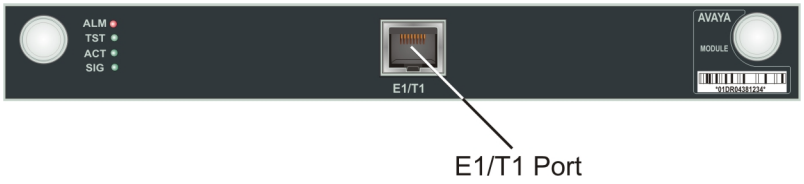


Figure 24: The MM340 media module

Procedure

Plug the WAN line into the E1/T1 port, marked E1/T1, on the MM340 media module

Use an unshielded twisted pair cable, straight or crossover, depending on the WAN equipment.

Connecting an Ethernet WAN link

About this task

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

Connecting an external router to the Branch Gateway

About this task

Procedure

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

- The ETH WAN ports on the Branch Gateway front panel
- The ETH LAN ports on the Branch Gateway front panel

Coupled Bonding Conductor installations

The Coupled Bonding Conductor (CBC) provides mutual inductance coupling between the CBC and the telephone cables that are exposed to lightning. The conductor can be a 10 AWG (4 mm^2) wire tie wrapped to the exposed cables, a metal cable shield around the exposed cables, or six spare pairs from the exposed cable. In a high-rise building, connect the CBC to an approved building ground on each floor.

Related topics:

Installing the CBC on page 57

Installing the CBC

About this task

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

Procedure

1. Connect one end of the conductor to a telephone cable building entrance protector ground that is connected to an approved ground.
2. Route the rest of the conductor next to the exposed telephone cables being protected until they reach the cross-connect nearest to the telephone system.
3. Terminate the other end to the single-point ground block provided for the telephone system.

Result

Note:

Position the non-exposed telephone cables at least 12 in (30.5 cm) away from exposed telephone cables whenever possible.

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 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 can be operated in either a “normally closed” or “normally open” state. The contact closures can control auxiliary devices such as devices that automatically lock or unlock doors or voice recording units. The CCA port can be configured so that the connected devices can be controlled by an end device, such as a telephone. For example, a user can unlock a door by keying a sequence into a telephone keypad.

Related topics:

Installing the contact closure on page 58

Installing the contact closure

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 that will be activated and deactivated by the Contact Closure relays.
2. Note which device is connected to each relay.

   You will need this information for configuration.
3. Connect the Avaya Partner Contact Closure adjunct box to the CC port on the Branch Gateway front panel.

   Use a 24 gauge minimum telephone wire, no longer than 200 ft, with a standard four wire RJ-11 connector.

808A Emergency Transfer Panel and associated telephones installations

The ETR feature provides basic telephone services in the event of system failure, such as a power outage or a failed connection to the MGC. The ETR feature can be used in conjunction with an analog media module (MM711, MM714, MM714B, or MM716). The ETR panel provides up to five incoming Central Office (CO) trunk loops to 5 selected G450 analog lines. Thus, one ETR panel supports up to five emergency lines. You can cascade a second ETR panel,

providing support for up to 10 emergency analog phones. ETR is activated automatically upon system failure by closing the tip/ring contacts between the analog lines and the analog trunks. When ETR is activated, all calls are directed by the analog relays between the outside lines and the analog telephones. A current-loop detection circuit prevents ongoing calls from being disconnected when normal functioning resumes. If a call is in progress on an outside line when the problem ends, the call continues. The trunk port and analog line port passing through the ETR panel do not start to operate until the active call ends.

For information on installing the 808A Emergency Transfer Panel, see *808A Emergency Transfer Panel Installation Instructions*, 03-602518, which ships with the Emergency Transfer Panel.

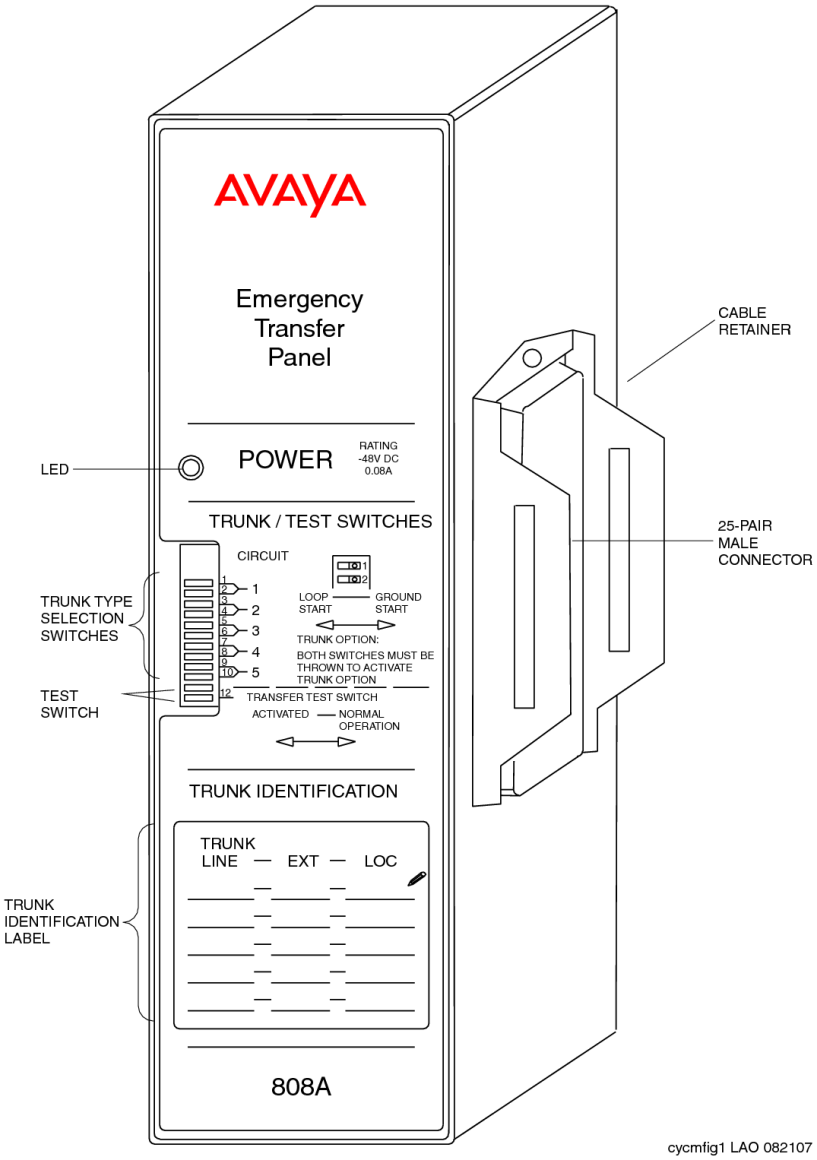


Figure 25: 808A Emergency Transfer Panel

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

Modems for remote access

You can connect a modem to the Branch Gateway to enable configuration from a remote location. A serial modem connected to the Branch Gateway can also be used for the modem dial backup feature, which provides a redundant connectivity with a remote primary Media Gateway Controller (MGC). Modem dial backup provides better survivability than switching to a secondary MGC, since more features are preserved.

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

Note:

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

Note:

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

Related topics:

Gateways without S8300 modem connections on page 61
Branch Gateways with S8300 USB modems on page 66

Gateways without S8300 modem connections

You can either connect a serial modem to the Console port, or you can connect a USB modem to either of the two USB ports on the Gateway front panel.

Related topics:

Connecting and enabling a serial modem on page 62
Connecting and enabling a USB modem (Branch Gateway without S8300) on page 63
Testing the modem connection (Branch Gateway without S8300) on page 66

Connecting and enabling a serial modem

Procedure

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

   Note:

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

   Note:

   You can install firmware upgrades for the Banch Gateway and media modules from CD-ROM or downloaded from the Web.
2. Download Gateway Installation Wizard (GIW) from the Avaya Support website (support.avaya.com/avayaiw) to the laptop computer.
   The laptop must be running Windows 2000, Windows 2003 server, or Windows XP to support GIW.
3. Plug one end of the provided flat RJ-45 to RJ-45 cable into the provided DB-9 adapter.
4. Plug the RJ-45 connector at the other end of the cable into the Console port of the Banch Gateway.
5. Plug the DB-9 end of the flat cable into the COM port of the laptop computer.
6. From your laptop computer, double-click the GIW icon to run GIW.
   The Overview screen appears.
7. Click **Continue**.
   The Gateway Connection Details screen appears.
8. Choose **Select if this is any Gateway other than G430**.
9. Click **Continue**.
   The Media Gateway Wizard Usage Options screen appears.
10. Select **Enable the modem for remote installation**.
11. Click **Continue**.
    The Media Gateway Modem Type Selection screen appears.

12. Click **Continue** until the Modem Type Selection screen appears.
13. Select **Serial Modem**.
14. Click **Continue**.
    The Media Gateway Serial Modem Configuration screen appears.
15. In the IP Address field, enter the RAS IP address of the modem obtained using the ART tool.
    See Running the Automatic Registration Tool (ART) for the RAS IP address on page 14.
16. Fill in the remaining modem information fields.
17. Select the authentication method:
    - If you have an Avaya Service contract, check **Enable ASG Authentication** to enable remote access to the device.
    - If you do not have an Avaya Service contract:
      - Check **Enable CHAP Authentication**.
      - In the **CHAP Secret** field, enter the CHAP secret key obtained using the ART tool. See Running the Automatic Registration Tool (ART) for the RAS IP address on page 14.
      - In the **Confirm CHAP Secret** field, re-enter the CHAP secret key.
18. **Click Continue**.
    The Connect Modem screen appears.
19. Click **Finish**.
20. Connect the serial modem to a working telephone line.
21. Connect the provided DB-25 adapter to the modem.
22. Disconnect the flat cable from the COM port of the laptop computer.
23. Connect the flat cable to the DB-25 connector on the modem.

Connecting and enabling a USB modem (Branch Gateway without S8300)

About this task

You can enable a USB modem on athe USB port on the Branch Gateway front panel. See USB modems supported by the Bracnh Gateway on page 164 for a list of the USB modems supported by the Bracnh Gateway

Note:

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

Procedure

1. Prepare a PC with a CD-ROM drive, SSH client software, and a TFTP server on the network.

   This may be needed for installing software and firmware upgrades.

   Note:

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

   Note:

   Firmware upgrades for the Branch Gateway and media modules can either be installed from CD—ROM or downloaded from the Web.

2. Download GIW (Gateway Installation Wizard) from the Avaya Support website support.avaya.comto the laptop computer.

   The laptop must be running Windows 2000, Windows 2003 server, or Windows XP to support GIW.

3. Set the laptop's TCP/IP properties as follows:

   - IP address: 192.11.13.5
   - Subnet mask: 255.255.255.252
   - Disable DNS service
   - Disable WINS Resolution

4. Disable the proxy server in the laptop’s Internet browser settings.
5. Connect an Ethernet cable from the laptop computer to the G430 Services port.
6. Plug one end of the provided flat RJ-45 to RJ-45 cable into the provided DB-9 adapter.
7. Plug the RJ-45 connector at the other end of the cable into the Console port of the Branch Gateway.
8. Plug the DB-9 end of the flat cable into the COM port of the laptop computer.
9. From your laptop computer, double-click the GIW icon to run GIW.

   The Overview screen appears.

10. Click **Continue**.

    The Gateway Connection Details screen appears.

11. Choose **Select if this is any Gateway other than G430**.

12. Enter your Username and Password.
13. Click **Continue**.
    The Media Gateway Wizard Usage Options screen appears.
14. Select **Enable the modem for remote installation**.
15. Click **Continue**.
    The Media Gateway Modem Type Selection screen appears.
16. Click **Continue** until the Modem Type Selection screen appears.
17. Select **USB Modem**.
18. Click **Continue**.
    The Media Gateway USB Modem Configuration screen appears.
19. In the PPP IP Address field, enter the RAS IP address of the modem obtained using the ART tool.
    See Running the Automatic Registration Tool (ART) for the RAS IP address on page 14.
20. Enter the PPP Subnet Mask.
21. Select the authentication method:
    - If you have an Avaya Service contract, check **Enable ASG Authentication** to enable remote access to the device.
    - If you do not have an Avaya Service contract:
      - Check **Enable CHAP Authentication**.
      - In the **CHAP Secret** field, enter the CHAP secret key obtained using the ART tool. See Running the Automatic Registration Tool (ART) for the RAS IP address on page 14.
      - In the **Confirm CHAP Secret** field, re-enter the CHAP secret key.
22. Click **Continue**.
    The Connect Modem screen appears.
23. From the Connect Modem screen, click **Finish** to exit the Gateway Installation Wizard.
24. Click **Continue** until you exit the Gateway Installation Wizard.
25. Click **Finish**.
26. Connect a USB modem to a working telephone line.
27. Connect one end of a USB cable to the modem.
28. Connect the other end of the USB cable to athe USB port on the Branch Gateway front panel.

Testing the modem connection (Branch Gateway without S8300)

About this task

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

Procedure

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

Branch Gateways with S8300 USB modems

You can connect a USB modem to a USB port on the S8300 front panel. See USB modems supported by the S8300 on page 164 for a list of the USB modems supported by the S8300.

Related topics:

Maintenance web pages on page 66
Branch Gateways with S8300 modem connections on page 68
Testing the modem connection (Branch Gateway with S8300) on page 68
Connecting the USB CD-ROM drive on page 69

Maintenance web pages

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

Related topics:

Changing the modem settings on the Configure Server Maintenance Web Page on page 67

Changing the modem settings on the Configure Server Maintenance Web Page

Procedure

1. Select
   Configure Server
   from the left-hand menu on the Maintenance web page.
   The Back Up Data page appears.
2. Follow the on-screen instructions to back up the current data.
3. Click
   Continue
   .
4. Select
   Configure individual services
   .
5. Click
   Continue
   .
6. From the left navigation menu, click
   Set Modem Interface
   .
   The Set Modem Interface page appears.
7. Enter the RAS IP address you obtained using the ART tool.
   See Running the Automatic Registration Tool (ART) for the RAS IP address on page 14.
8. Click
   Change modem settings
   .
9. Click
   Continue
   .
10. Click
    Close Window
    .

Result

Note:

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

Branch Gateways with S8300 modem connections

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

Note:

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

Related topics:

Connecting and enabling the modem on page 68

Connecting and enabling the modem

Procedure

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

   The Modem page displays.
4. Select **Enable modem for unlimited incoming calls**.
5. Click **Submit**.

Testing the modem connection (Branch Gateway with S8300)

Procedure

1. Setup a dialup connection on a remote PC with the following settings:
   - Automatically detect settings.
   - No Username, Password, or Domain.

    - Security > Show Terminal Window.
2. Dial in to the modem from the remote PC.
3. When prompted, provide the rasaccess login and password in the Terminal Window.
4. Close the Terminal Window to complete the connection.
5. Activate an SSH session.
6. Login valid authentication to the Linux CLI.

Connecting the USB CD-ROM drive

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

Chapter 5: Configuring the Branch Gateway

Branch Gateway configuration

The Branch Gateway requires software configuration. The Branch Gateway can be configured 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 using the CLI, see Administration for the Avaya Branch Gateway G450, 03-602055. For detailed information on CLI commands, see the Avaya Branch Gateway G450 CLI Reference, 03-602056.

The Branch Gateway can be accessed:

- At the customer site via a laptop connected to the Console port or Services port of the Branch Gateway. For information about connecting a laptop to the Services port, see Connecting a computer to the Services port.
- From a remote location via a modem. For information about connecting and enabling a modem, see Modems for remote access on page 61.
- Remotely through the network. For information about preparing a newly installed Branch Gateway for configuration via the network, see Configuring basic gateway connectivity on page 71.

Related topics:

Configuring basic Branch Gateway connectivity on page 71

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.

Note:

The installation script is supported from Branch Gateway firmware version 29.22.x.

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 computer to the Branch Gateway Services port, using an Ethernet cable.
4. SSH to 192.11.13.6.
5. At the prompt, enter the default username: `root` and password: `rootroot0`.
6. At the prompt, configure a new password.
7. At the prompt, enter `y` to configure basic gateway connectivity.

   Note:

   If you enter `n` but then change your mind, you can use the **`script-config`** CLI command to run the installation script, so long as you have not saved any configuration changes you may have made.
8. You are prompted to configure the following parameters.

   For each parameter, you can enter a value, or press Enter to accept the default value shown in square brackets:
   - VLAN number
   - IPv4 enabled or disabled
   - 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.

9. Connect the Ethernet port to the network to enable remote access to the gateway.

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

Chapter 6: After installation

After installation

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

Related topics:

Roadmap for post installation on page 75
Installation testing on page 75
Removing the installation equipment on page 79

Roadmap for post installation

Perform these post-installation procedures tin 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.

Related topics:

Testing data connectivity on page 76
Testing telephones on page 76
Testing trunks on page 76
Testing LSP failover on page 76

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 Procedures for Avaya Aura® Communication Manager, Media Gateways and Servers*, 03-300432.

Testing LSP failover

About this task

If you have an S8300 Server installed in the Branch Gateway and configured as an LSP, 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 both fail, then the Branch Gateway enters SLS mode.

Procedure

1. Verify that valid translations are file synchronized to the LSP by logging into Avaya Aura® Communication Manager from the LSP and listing either stations or trunks, see *Administering Avaya Aura®Communication Manager*, 03-300509.

   Verify that the list of stations or trunks is valid. If the files are not synchronized, verify that you have correctly configured the required IP address(es) for the primary controller(s) (MGC). If you are using Avaya IW to configure the Branch Gateway, the following are key actions that must be done in the wizard to ensure correct IP address configuration:

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

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

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

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

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

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

   Note:

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

2. If valid translations are not file synchronized to the LSP, do the following:

   a. From a SAT session run from the primary controller, verify that the LSP node-name and IP address are correctly entered.

b. Use the **`save translation lsp`** command to start the file synchronization process.
c. Log in again to Avaya Aura® Communication Manager from the LSP and list either stations or trunks.
d. Verify that the list of stations or trunks is valid.

3. Disconnect the Branch Gateway from the primary controller, ensuring that all telephones are still connected or have network connectivity to the Branch Gateway.
4. Verify that calls can be made between local telephones using the locally connected outside lines to the Branch Gateway.

Result

Note:

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

Related topics:

IP addresses and controllers on page 78

IP addresses and controllers

Primary media gateway controller	IP addresses to configure
S8300	The IP address of the primary S8300
S8400	The IP address of the S8400’s C-LAN or the IP address of an Ethernet port on the S8400 configured for processor Ethernet connections
S8500	The IP address of the S8500’s C-LAN or the IP address of an Ethernet port on the S8500 configured for processor Ethernet connections
S8510	The IP address of the S8510’s C-LAN or the IP address of an Ethernet port on the S8510 configured for processor Ethernet connections
[1]	The IP address of the S8700’s C-LAN and the IP address of alternate C-LAN boards connected to the S8700 (Server A LAN, Server B LAN)
S8710	The IP address of the S8710’s C-LAN and the IP address of alternate C-LAN boards connected to the S8710

[1]

Primary media gateway controller	IP addresses to configure
S8720	The IP address of the S8720's C-LAN and the IP address of alternate C-LAN boards connected to the S8720
S8730	The IP address of the S8730's C-LAN and the IP address of alternate C-LAN boards connected to the S8730

Removing the installation equipment

About this task

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

Note:

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

Chapter 7: Adding media modules and devices

Media module and device additions

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

Related topics:

Media module additions on page 81
Telephone additions on page 82
Trunk additions on page 84

Media module additions

Various media modules including voice modules or WAN modules can be added to the Branch Gateway.

Related topics:

Voice module additions on page 81
WAN module additions on page 82

Voice module additions

You can hot-swap voice modules. This means that you can add or remove a voice module in the Branch Gateway 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 82 and Adding a trunk on page 84.

Some configuration of the Avaya Aura® Communication Manager is necessary when you install an MM710, MM710B, MM720, MM721, or MM722 media module. See *Administrator's Guide for Avaya Aura® Communication Manager*, 555-233-506. 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 G450 CLI Reference*.

WAN module additions

You can hot-swap WAN modules. This means you can add or remove a WAN module in the Branch Gateway while the system is running, but the Branch Gateway resets when you add or remove the module. However, hot insertion and removal is not recommended in most cases. Because hot insertion or removal resets the Branch Gateway, any translation and other data that is in the running configuration but has not been saved to the startup configuration will be lost.

There is no configuration necessary when you add or remove a WAN module. Configuration is only necessary when you add WAN lines to the new module. See Adding a WAN line on page 86.

Telephone additions

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

Related topics:

Telephone connections on page 82
Configuration of telephones on Communication Manager on page 83
Testing the telephone on page 83

Telephone connections

To connect a new telephone, see the following sections:

- Connecting an IP telephone on page 46
- Connecting an analog telephone on page 49
- Connecting a DCP telephone to an MM312, MM712, or MM717 media module on page 50

Configuration of telephones on Communication Manager

Standalone:

- Configuration may be performed on site by connecting a laptop computer to the Console port or Services port of the Branch Gateway or S8300, or remotely via a modem connected to the Branch Gateway or S8300.
- LSP: Configuration is done on the primary Communication Manager server.

For information about connecting a laptop to the Services port, see Connecting a computer to the Services port. For information about preparing a modem, see Modems for remote access on page 61. For information about configuration, see Branch Gateway configuration on page 71.

Related topics:

Recording of telephone information for software configuration on page 83

Recording of telephone information for software configuration

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

- Name and location of the owner of the telephone
- Model number of the telephone
- Extension of the telephone
- Slot and port number on the 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.

Related topics:

Trunk ordering on page 84

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

Related topics:

Special considerations when ordering an analog trunk on page 84

Special considerations when ordering an analog trunk

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

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

  Note:

  If you use the MM714B with ground start, you must use a ground start button for ETR.
- Request conditioned lines to ensure satisfactory voice quality and trunking interactions

Connecting the trunk

Trunk configurations on Communication Manager

- Standalone: Configuration may be performed on site by connecting a laptop computer to the Console port or Services port of the Branch Gateway or S8300, or remotely via a modem connected to the Branch Gateway.
- LSP: Configuration is done on the primary Communication Manager server.

Note:

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

For information about connecting a laptop to the Services port, see Connecting a computer to the Services port. For information about preparing a modem, see Modems for remote access on page 61. For information about configuration, see Branch Gateway configuration on page 71.

Related topics:

Trunk information recordings for software configuration on page 85

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 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.

WAN line additions

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

Related topics:

WAN line ordering on page 86
WAN line connections on page 86
WAN line configuration on page 86
Testing the WAN link on page 86

WAN line ordering

If you need to order the WAN 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.

WAN line connections

To connect a WAN line, see Connecting to the Wide Area Network (WAN) on page 55.

WAN line configuration

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

For information about connecting a laptop to the Services port, see Connecting a server. For information about preparing a modem, see Chapter 4: Connecting and enabling a modem for remote access on page 61. For information about configuration, see Chapter 5: Configuring the Branch Gateway on page 71.

Related topics:

WAN information recordings for software configuration on page 86

WAN information recordings for software configuration

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

- Slot and port number on the Branch Gateway to which the WAN line connects

Testing the WAN link

About this task

After installation of the WAN line is complete, test the link by verifying that the SIG LED for the port to which the link connects is lit. It is also recommended that you ping the IP address of a device using the WAN line and perform 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 58.

Chapter 8: Upgrading and replacing Field Replaceable Units

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:

There are two hardware versions of G450, referred to as G450 1.x and G450 2.x and greater.

- On G450 1.x, the ASB button is to the right of the RST button.
- On G450 2.x and greater, the RST button is above the ASB button.

In cases where the instructions differ according to the G450 version, instructions are given for both versions.

Related topics:

Branch Gateway main board modules on page 89
Replacing the fan tray on page 108
Replacing a power supply unit on page 109

Branch Gateway main board modules

You can add or remove memory modules and VoIP modules in the Branch Gateway main board. To do so, you must pull out the Branch Gateway main board. The Branch Gateway supports hot insertion and removal of the main board without power drop. However, all services are suspended while the Branch Gateway main board is out, and all calls passing through the Branch Gateway are disconnected. Any translation and other data that is in the running configuration but has not been saved to the startup configuration is lost.

Electrostatic alert:

Do not touch any components on the printed circuit board.

Electrostatic alert:

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

Caution:

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

Note:

Consult your project manager before adding or removing memory modules or VoIP modules in the Branch Gateway.

Related topics:

[Removing and inserting the Branch Gateway main board](#) on page 90
[Inserting or replacing a RAM card in the G450](#) on page 91
[Adding or removing VoIP modules: MP20 and MP80](#) on page 95
[Adding and removing MP160](#) on page 100
[Compact flash memory cards](#) on page 104

Removing and inserting the Branch Gateway main board

Procedure

1. To remove the Branch Gateway main board:
   a. Unscrew the two captive screws, one at each side of the Branch Gateway main board front panel.
   b. Open the latches on both sides of the main board.
   c. Grasp the latches and pull out the main board from its slot.
   d. Place the main board carefully on a table.
2. To insert the Branch Gateway main board:
   a. Open the latches on both sides of the slot.
   b. Insert the Branch Gateway main board vertically into the slot.
   c. Push the main board in until the latches begin to close.
   d. Close and tighten the two captive screws on the front panel and then tighten the latches.
   e. Use the **`show platform mainboard`** CLI command to make sure the Branch Gateway is working properly.

Result

Figure 26: Removing and inserting the Branch Gateway main board

Inserting or replacing a RAM card in the G450

About this task

Note:

There are two hardware versions of the G450, referred to as G450 1.x and G450 2.x. G450 1.x is the G450 version with hardware suffix 1, and the G450 2.x is the G450 version with hardware suffix 2. The hardware suffix of the G450 is printed on the label displayed on the rear of the G450 chassis.

In cases where the instructions differ depending on the G450 version, instructions are given for both versions.

Warning:

Do not insert an additional RAM card into the second slot on the G450 2.x.

The G450 has two RAM slots. The basic configuration includes one 256 MB RAM card.

The slots are located on the G450 main board. You must pull out the main board to remove or insert a memory card. The G450 supports hot insertion and removal of the main board without power drop. However, all services are suspended while the G450 main board is out, and all calls passing through the gateway are disconnected. Any translation and other data that is in the running configuration but has not been saved to the startup configuration is lost.

To increase RAM memory in the gateway:

- In the G450 1.x, insert the 256 MB RAM card provided in the kit into the second RAM slot.
- In the G450 2.x, remove the RAM card from the main board and replace it with the 512 MB RAM card provided in the kit .

Procedure

Upgrade RAM memory:

- In the G450 1.x, see Inserting a G450 1.x RAM card on page 92.

- In the G450 2.x, see Replacing the G450 2.x RAM card on page 93.

Related topics:

Inserting a G450 1.x RAM card on page 92
Replacing the G450 2.x RAM card on page 93

Inserting a G450 1.x RAM card

About this task

Electrostatic alert:

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

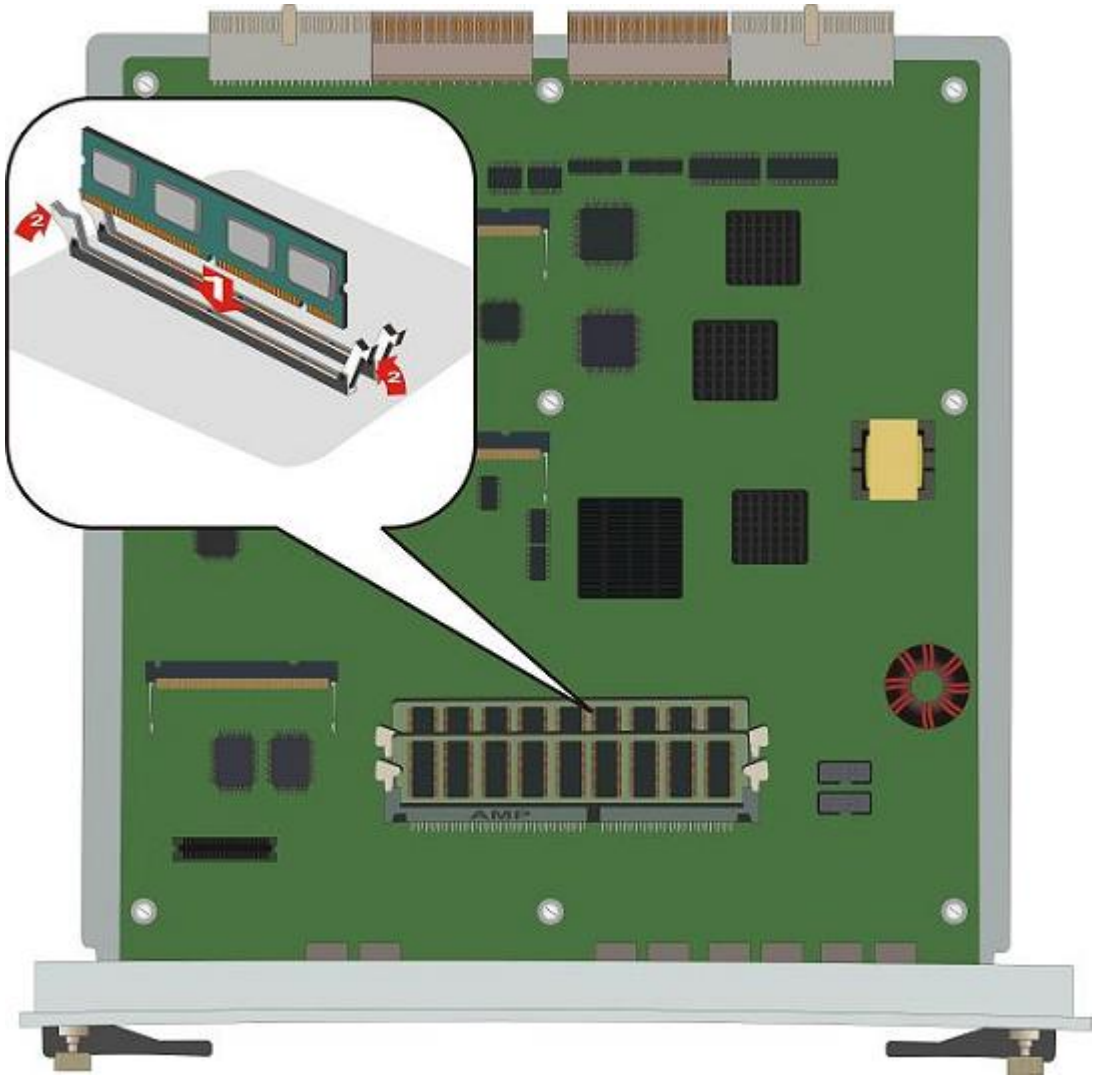
Caution:

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

Procedure

1. Locate the empty RAM slot, as show in the figure.
2. Make sure the white latches at either side of the empty RAM slot are open outwards.
3. Insert the 256 MB RAM card provided in the kit into the RAM slot and push down, until the two latches on either side of the card lock into place.

   To remove a RAM card, open the latches on both sides of the RAM slot housing the RAM card. The RAM card lifts up. Pull out the RAM card.



Replacing the G450 2.x RAM card

About this task

Electrostatic alert:

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

Warning:

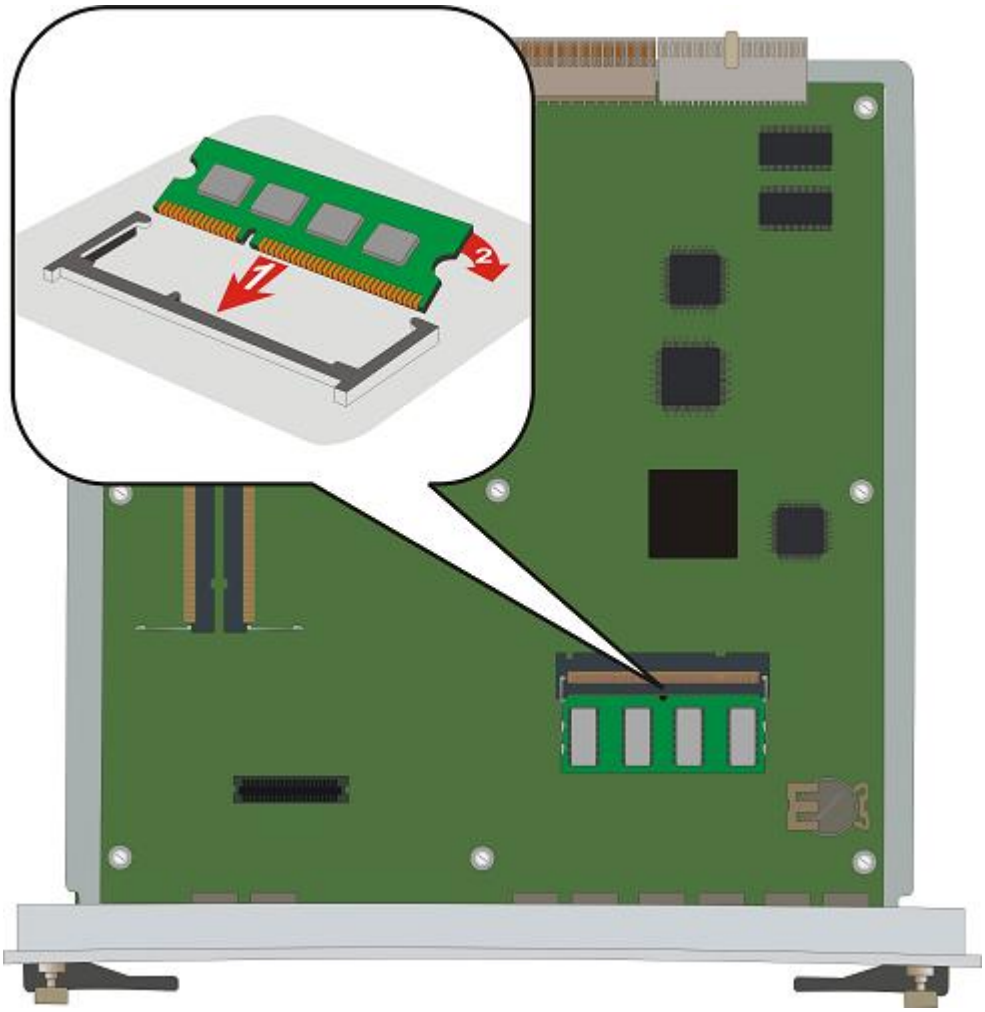
Insert the RAM card into the *first* RAM slot (SODIMM A) *only*.

Procedure

1. Locate the RAM slot holding the RAM card, as shown in the figure.
2. Open the latches on both sides of the RAM slot. The RAM card lifts up.
3. Pull out the 256 RAM card.

   Important:

   Remove the RAM card in SODIMM slot A.You can only replace the RAM card in SODIMM slot A, you cannot add an extra card in SODIMM slot B.
4. Insert the 512 RAM card provided in the kit, or a replacement 256 RAM card, 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.



Adding or removing VoIP modules: MP20 and MP80

About this task

The G450 main board has four slots for VoIP engines. Each slot can accommodate either an MP20 (Media Processor 20) module or an MP80 (Media Processor 80) module. An MP20 provides 25 channels for G.711 and G.726 and 20 channels for G.729, and an MP80 provides 80 channels.

The G450 supports a maximum of 320 active channels. Therefore, any combination of MP80 and MP20 in the four DSP slots can be supported.

Note:

The G450 prior to release 5.2.1 supports up to 240 channels.

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.

There is no configuration necessary when you install an MP20 or MP80 module.

Procedure

1. To insert an MP20 or MP80 module:
   a. Locate the MP20 or MP80 module slot.

      The location differs depending on the hardware version of the G450 (see the figure on page 96 and the figure on page 97).

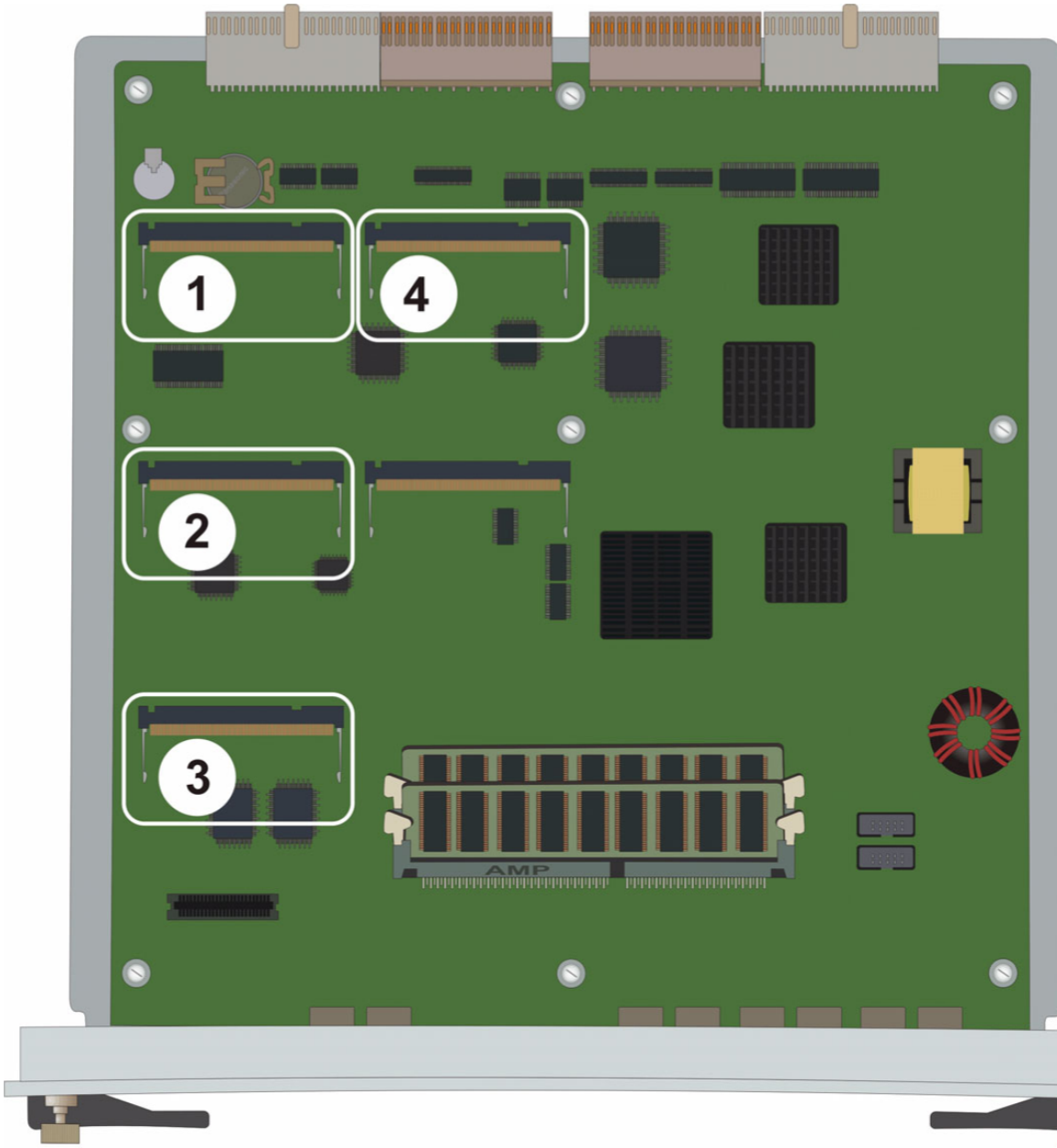


Figure 27: Location of MP20 and MP80 module slots in a G450 1.x

Table 4: Figure notes:

i. MP20 or MP80 module slot	i. MP20 or MP80 module slot
ii. MP20 or MP80 module slot	ii. MP20 or MP80 module slot

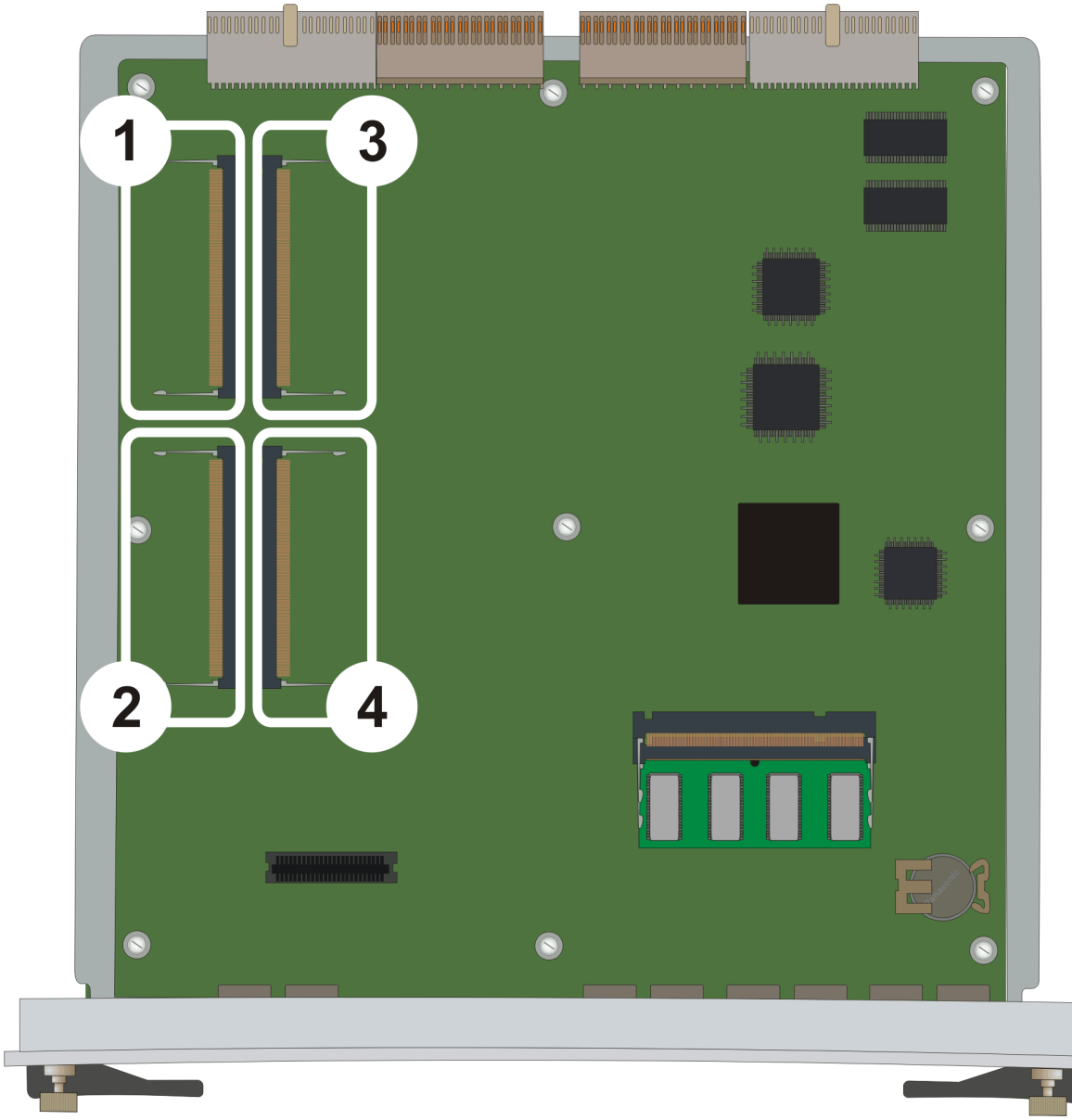


Figure 28: Location of MP20 and MP80 module slots in a G450 2.x

Table 5: Figure notes:

i. MP20 or MP80 module slot	i. MP20 or MP80 module slot
ii. MP20 or MP80 module slot	ii. MP20 or MP80 module slot

b. Position the MP20 or MP80 module at a 45 degree angle to the main board, and start inserting it into an MP20 or MP80 slot (see the figure on page 98 and the figure on page 99).

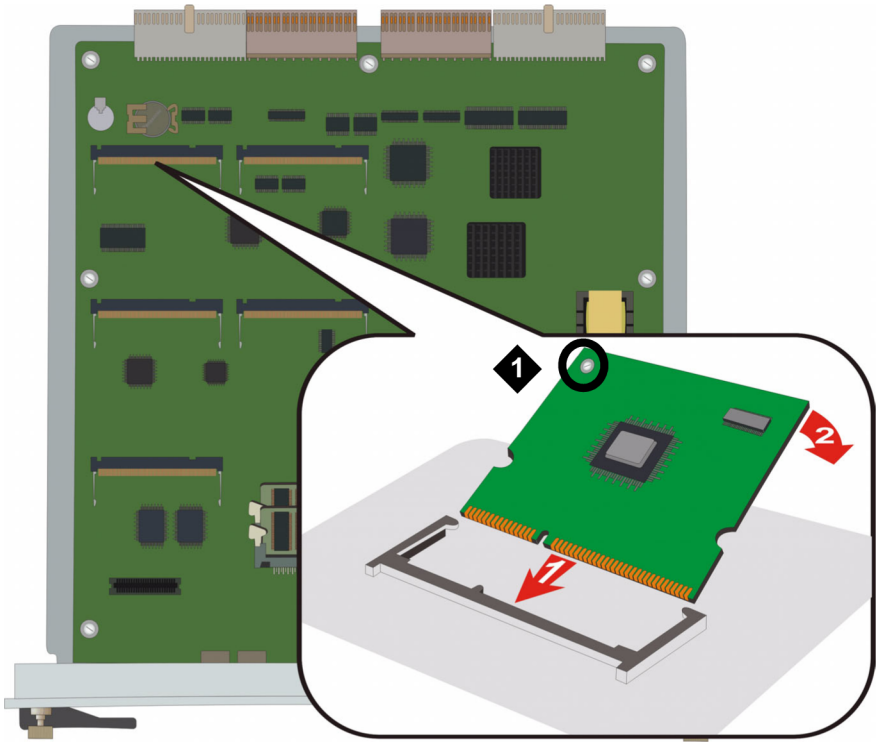


Figure 29: Adding or removing an MP20 or MP80 module in a G450 1.x

Table 6: Figure notes:

	VoIP module locking screw

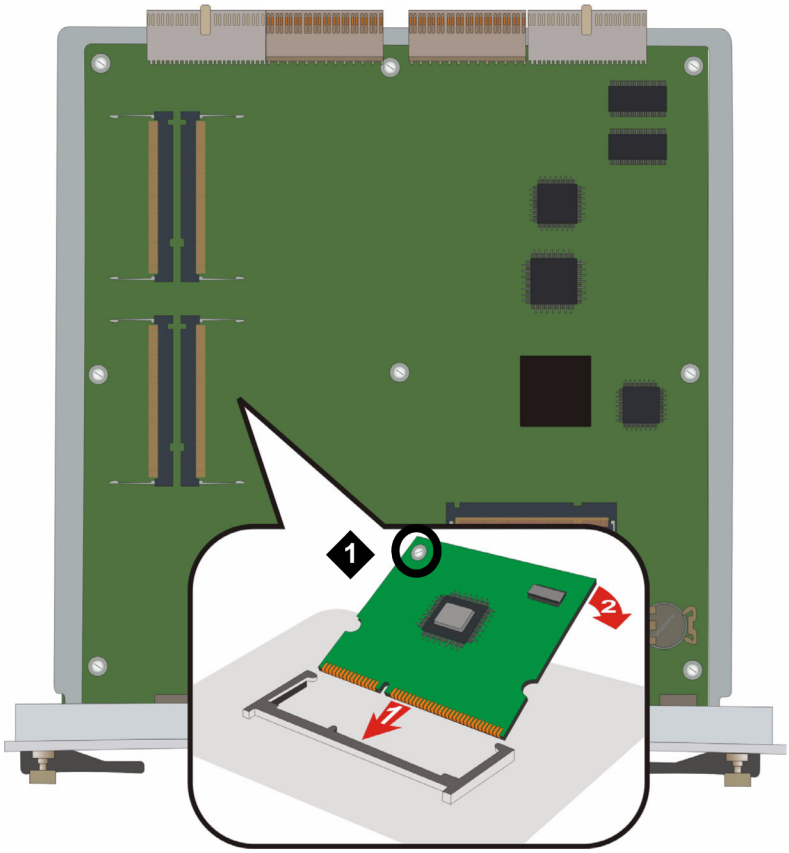


Figure 30: Adding or removing an MP20 or MP80 module in a G450 2.x

Table 7: Figure notes:

	VoIP module locking screw

c. Push the module in all the way. Do not use too much force.
d. Flatten the module so it is flush with the main board.

   The latches at both sides click shut.
e. Tighten the locking screw affixed to the VoIP module.

   This secures the VoIP module to the motherboard.
f. After powering up, use the **`show platform mainboard`** CLI command to make sure everything is OK.

2. To remove an MP20 or MP80 module:
   a. Unscrew the locking screw attaching the VoIP module to the motherboard (see the figure on page 98 and the figure on page 99).
   b. Open the latches on both sides of the module slot.

      The module lifts up.
   c. Pull out the module.

Touch the module only at the edges.

Adding and removing MP160

Before you begin

The G450 main board has four slots for VoIP engines. You can install up to two MP160s (Media Processor 160). An MP160 provides 160 channels for voice transport. Alternatively, if no standard voice is required, a maximum of 120 channels of V.150.1 call traffic is supported. A combination of voice calls and V.150.1 calls is supported per the Avaya configuration guidelines.

Note:

G450 supports up to 320 active channels for voice transport. You can install up to two MP160 modules, or a combination of Media Processor modules with a total of up to 320 channels for voice transport, for example, one MP160 and two MP80s.

See the table below for permitted combinations of Media Processor modules:

Combination of cards	MP20	MP80	MP160
Combination #1	-	-	1 or 2
Combination #2	1 or 2	-	1
Combination #3	-	1 or 2	1
Combination #4	1	1	1

Important:

You can only install MP160 in slots 2 and 4 on the G450 1.x or slots 1 and 2 on the G450 2.x. (see Figure 32: Location of DSP module slots in a G450 1.x on page 102 and Figure 33: Location of DSP module slots in a G450 2.x on page 103) On the G450 1.x, the ASB button is to the *right* of the RST button. On the G450 2.x, the RST button is *above* the ASB button.

You can also use the `show system` command in the command line interface to identify the mainboard HW vintage (version).

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 get bent or damaged if you handle the module roughly or if you misalign the module before forcing the module into position.

Caution:

Attach the correct standoff according to the hardware version of the G450. Using the wrong standoff will prevent you from installing the MP160 correctly.

About this task

You do not need to configure the G450 when you install an MP160. However, you must configure V.150.1 in Communication Manager in order to support V.150.1 applications such as modem-over-ip. See *Configuring V.150.1 on the Avaya G430 and G450 Branch Gateway*.

Procedure

1. Insert the provided plastic standoff in the hole.

   The standoff type differs depending on the hardware version of the G450. Ensure you use the correct standoff.

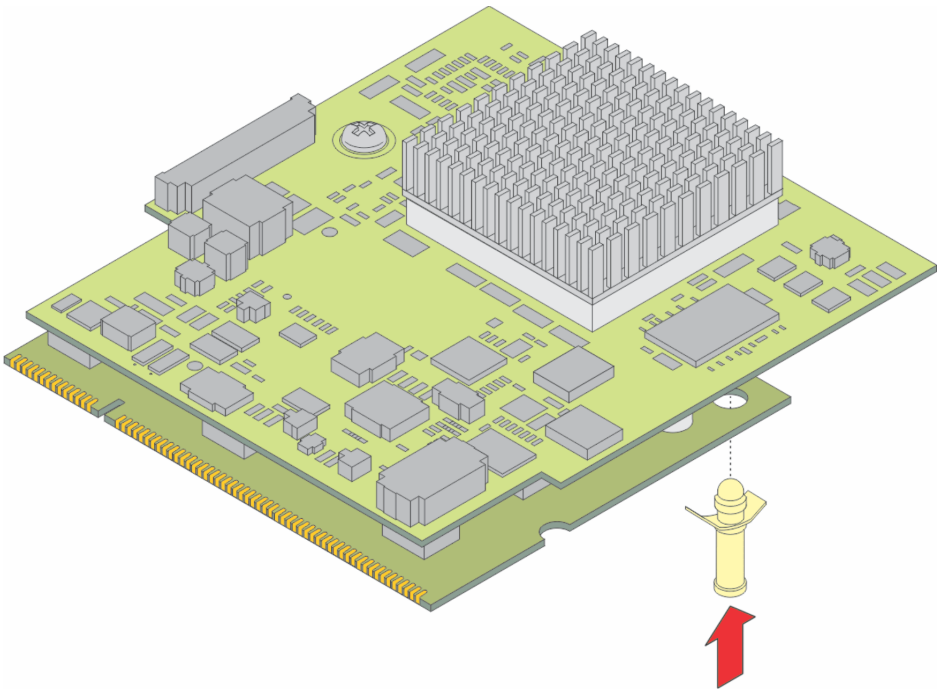


Figure 31: Location of Standoff on MP160

   - Use the *short* standoff For the G450 1.x.
   - Use the *long* standoff for the G450 2.x.

2. Locate the MP160 module slot. The location differs depending on the hardware version of the G450, see Figure 32: Location of DSP module slots in a G450 1.x on

page 102 and Figure 33: Location of DSP module slots in a G450 2.x on page 103.

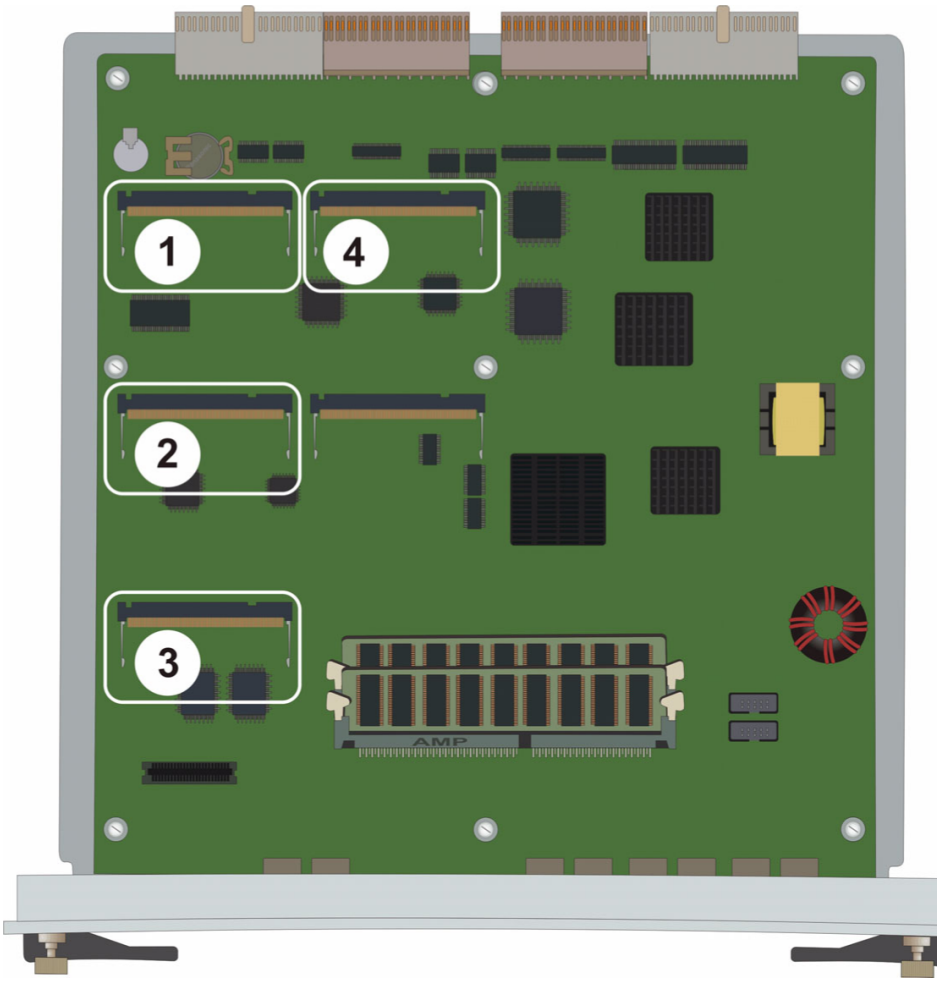


Figure 32: Location of DSP module slots in a G450 1.x

Table 8: Figure notes:

1. MP20 or MP80 module slot
2. MP20,MP80 or MP160 module slot
3. MP20 or MP80 module slot
4. MP20, MP80 or MP160 module slot

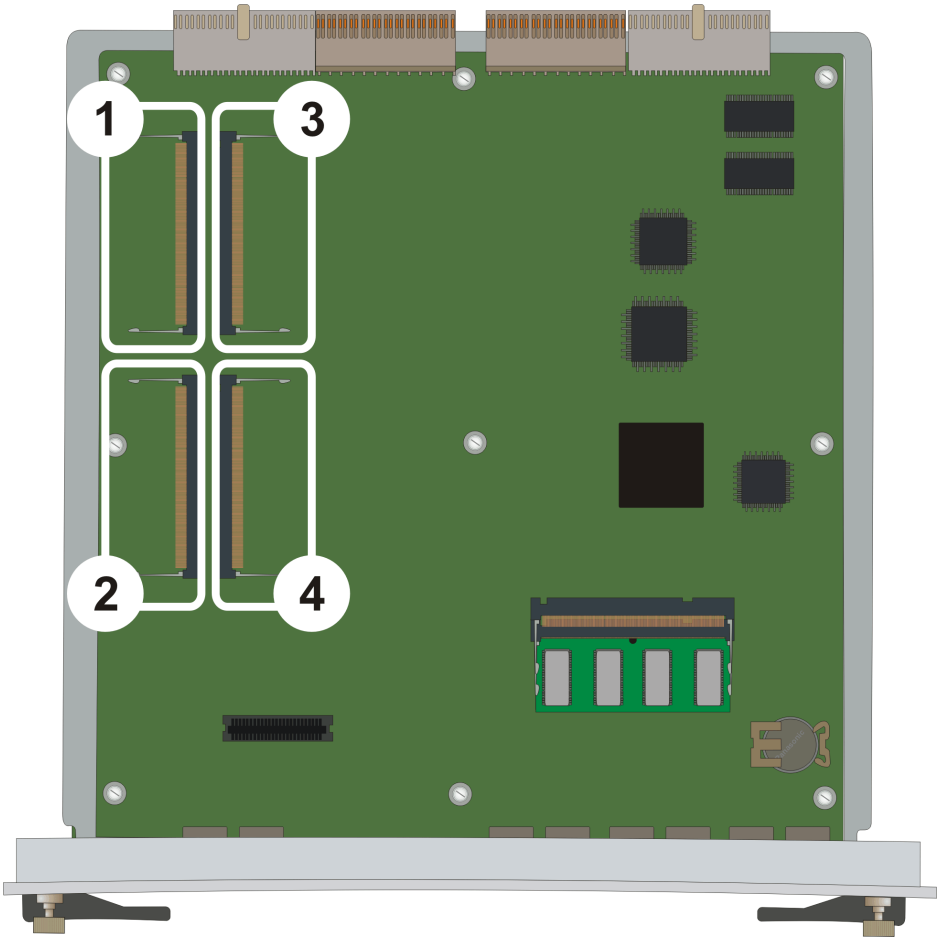


Figure 33: Location of DSP module slots in a G450 2.x

Table 9: Figure notes:

1. MP20, MP80 or MP160 module slot
2. MP20, MP80, or MP160 module slot
3. MP20 or MP80 module slot
4. MP20 or MP80 module slot

3. To insert the module into the slot, position the module at a 45 degree angle to the main board.

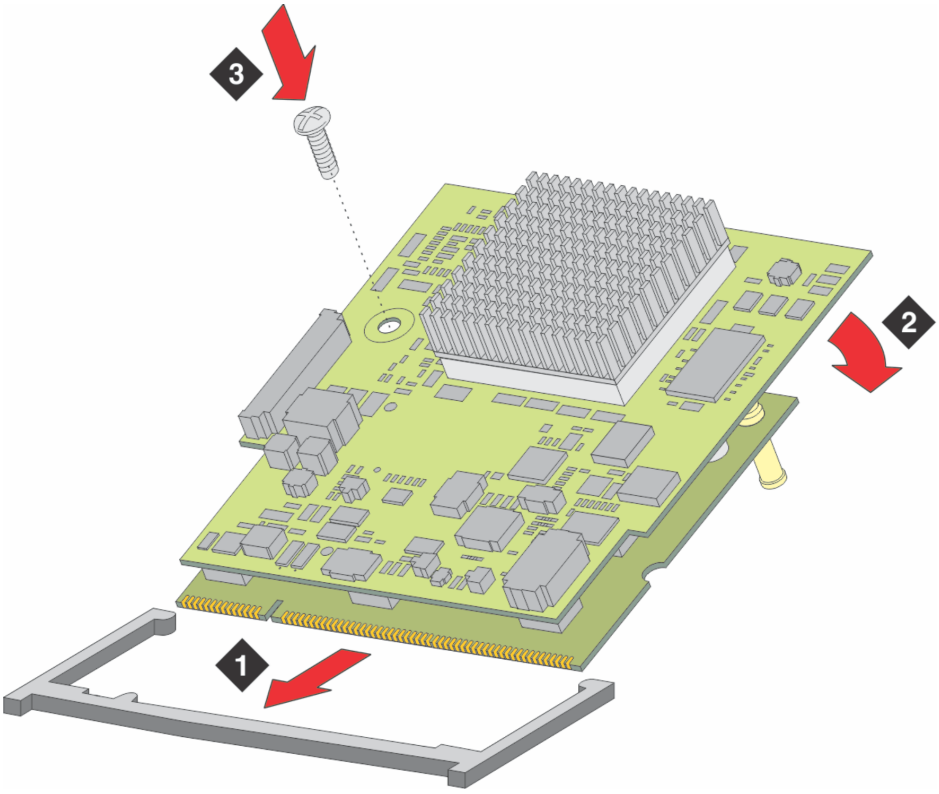


Figure 34: Adding or removing an MP160 in a G450

4. Push the module in all the way. Do not use too much force.
5. Flatten the module to flush with the main board.
   The latches at both sides click shut.
6. Insert the M3 X 5 screw provided with the kit.
7. Tighten the screw to secure the VoIP module to the motherboard

Next steps

After powering up, use the **`show platform mainboard`** CLI command to verify the installation.

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.

Related topics:

[Inserting a compact flash memory card](#) on page 105
[Compact flash memory card removals](#) on page 106

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 memory card so that the vendor name is facing up and the connector is pointing toward the Branch Gateway, and gently insert it into the compact flash slot.
3. After installing the compact flash memory card and the additional 256 MB RAM card, the announcement files are not automatically moved from the internal flash to the compact flash.

   To move them:

   a. Make sure the Branch Gateway is registered to Communication Manager.
   b. At the Communication Manager, set *enable CF* to `y` in the change media-gateway screen.
   c. In the SAT interface of the Communication Manager, enter **`enable announcement-board`**.
   d. The announcement files are copied from internal flash to the compact flash, and the yellow CARD IN USE LED associated with the compact flash flashes.
4. Use the **`show platform mainboard`** CLI command to verify that everything is OK.

   In the command output, the lower RAM slot is referred to as Memory socket #1, and the upper RAM slot is Memory socket #2.

   - A G450 1.x with increased memory displays, for example:

```
MEMORY SOCKET #1
------------------
Type                     : 256MB DDR SDRAM memory module with ECC
Serial Number            : 749f5c9f
Manufacture Part Num     : 9VDDT3272AY-335G4
Faults                   : No Fault Messages

MEMORY SOCKET #2
------------------
Type                     : 256MB DDR SDRAM memory module with ECC
Serial Number            : 749f5cb4
Manufacture Part Num     : 9VDDT3272AY-335G4
Faults                   : No Fault Messages
```

   - A G450 2.x with increased memory displays, for example:

```
MEMORY SOCKET #1
------------------
Type                     : 512MB DDR SDRAM memory module
Serial Number            : 0550749f
Manufacture Part Num     : 9VDDT3272AY-335G4
Faults                   : No Fault Messages

MEMORY SOCKET #2
------------------
```

```
Type                        : UNKNOWN
Serial Number               : UNKNOWN
Manufacture Part Num        : UNKNOWN
Faults                      : UNKNOWN
```

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 106 holding a different set of announcements
- Replacing a compact flash memory card while retaining The current announcements on page 107. 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 107

Related topics:

Swapping compact flash memory cards on page 106

Replacing a compact flash memory card while retaining the current announcements on page 107

Downgrading from a compact flash to internal flash memory on page 107

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 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 RAM to be lost.

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

5. At the SAT interface of the 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 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 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**.

   Note:

   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` in the change media-gateway screen.

Important:

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

Important:

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

   If you copied the announcement files one by one, you can restore them one by one using the CLI command **`copy ftp announcement-file`**.
8. Screw on the blank plate to cover the compact flash slot.

Replacing the fan tray

About this task

The fan system is field replaceable. It is mounted on a fan tray that can be replaced as one unit.

The Branch Gateway supports hot swap of the fan tray. There is no need to power down or reset the Branch Gateway when replacing a faulty fan tray unit.

Procedure

1. Prepare the new fan tray for insertion before removing the current the fan tray: take the new fan tray out of its package and place it nearby.

Important:

Replace the fan tray within one minute, to avoid overheating the Branch Gateway. If the Branch Gateway exceeds its allowed heat level, it shuts down.

If you remove and replace the fan tray, do not remove it again before waiting at least five minutes.

Figure 35: Replacing the fan tray

2. To remove the fan tray:
   a. Unscrew the two captive screws on the front panel of the fan tray.
   b. Grasp the screws and pull the fan tray out of its slot.
3. To insert the fan tray:
   a. Insert the fan tray all the way into the slot.
   b. Close and tighten the two captive screws on the front panel.

      The fans start operating immediately.
   c. Wait one minute and then use the **`show platform fans`** CLI command to make sure everything is OK.

Replacing a power supply unit

About this task

The Branch Gateway provides full redundant, load sharing power supply units (1 + 1). A single power supply unit provides enough power for any Branch Gateway configuration. If you choose to install two power supply units, the units operate in a load sharing mode.

The Branch Gateway supports hot swap of the power supply unit. Even if you have only one PSU unit installed, there is no need to turn off or reset the Branch Gateway when replacing a faulty power unit. You can install the replacement PSU in the second PWR slot, and it becomes the active PSU once you remove the faulty PSU.

Figure 36: Replacing a power supply unit

Procedure

1. To remove a power supply unit:
   a. Disconnect the Branch Gateway power cable from the mains socket.
   b. Disconnect the Branch Gateway power cable from the power connector, on the front panel of the power supply unit, at the rear of the Branch Gateway.
   c. Loosen the two captive screws, one on each side of the power supply unit.
   d. Grasp the two side handles and pull the power supply unit out of the slot.
2. To insert a power supply unit:
   a. Position the power supply unit before the opening and engage both sides of the unit in the interior guides.
   b. Slide the power supply unit slowly into the chassis, maintaining an even pressure to assure that the unit does not become twisted or disengaged from the guides.
   c. Close and tighten the two captive screws on the front panel.
   d. Connect the power cable to the power connector on the power supply unit.
   e. Plug the power cable into a mains socket.
   f. After turning on, use the **`show platform power`** CLI command to ensure everything is OK.

      The upper PSU is referred to as PSU #1 in the CLI, and the lower PSU is PSU #2.

Chapter 9: Upgrading the Avaya Aura Communication Manager software

Avaya Aura® Communication Manager upgrades

If your Branch Gateway includes an Avaya S8300 Server, it might be necessary to upgrade the Avaya Aura® Communication Manager software. Upgrading the software can be performed in one of the following ways:

- Remote configuration via Telnet — upgrade the software remotely via Telnet. In this scenario, a modem is required at the local site. See Chapter 4: Connecting and enabling a modem for remote access on page 61.
- Local configuration with S8300 Server — upgrade the software at the site, using a laptop computer and a CD-ROM drive connected to the S8300 Server
- Remote configuration via network — upgrade the software remotely via a network connection

Related topics:

Software upgrades using a CD-ROM drive on page 111
The Software Upgrade Manager on page 112

Software upgrades using a CD-ROM drive

The upgrade software is usually installed from a CD-ROM drive connected to the S8300. If the upgrade is performed locally, you might need to provide a laptop and a USB CD-ROM drive. If the upgrade is performed from a remote location, you must connect a USB CD-ROM drive to the S8300 and insert the upgrade CD-ROM in the CD-ROM drive. You also might need to connect a modem. This depends on the method used to perform the upgrade.

For a software upgrade on an Branch Gateway with an S8300 Server, use a USB modem. See USB modems supported by the S8300 on page 164 for a list of USB modems supported by the S8300.

Related topics:

Connecting the S8300 Server on page 112

Connecting the S8300 Server

About this task

Upgrade the software at the site, using a laptop computer and a CD-ROM drive connected to the S8300 Server.

Procedure

1. Connect the modem to a working telephone line.

   Note the telephone number of the line to which you connect the modem, so that you can provide the number to the technician who is performing or supervising the configuration.

2. Connect the USB modem to either of the two USB ports in the Avaya S8300 Server.

   Note:

   You may be required to enable the modem and port. For instructions on enabling the modem, see Chapter 4: Connecting and enabling a modem for remote access on page 61.

3. Connect a USB CD-ROM drive to the free USB port on the Avaya S8300 Server.
4. Insert the CD-ROM provided by Avaya into the CD-ROM drive.

The Software Upgrade Manager

You can upgrade the S8300 using the Software Update Manager or the Manage Software option in the Maintenance web pages. For information about upgrading S8300 firmware using the Software Upgrade Manager, see the *Avaya Software Update Manager User Guide*, 14-300168.

Chapter 10: Upgrading the Branch Gateway firmware

Branch Gateway firmware upgrades

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

Note:

The Branch Gateway firmware also includes the firmware for the MM340, and MM342 media modules.

Related topics:

Firmware upgrades using Software Update Manager on page 113
Firmware upgrades from the primary controller on page 114
Upgrading firmware using the CLI through FTP/TFTP on page 114
Upgrading Branch Gateway firmware using the CLI via a USB device on page 121

Firmware upgrades using Software Update Manager

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

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

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

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

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

Firmware upgrades from the primary controller

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

Note:

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

Upgrading firmware using the CLI through FTP/TFTP

About this task

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

Procedure

1. Prepare installation worksheets.

   See Preparing installation worksheets on page 117.

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

   For information about setting up a TFTP server, see Setting up a TFTP server on page 118.

   Note:

   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. Also, when opening an FTP connection to the S8300, all anonymous FTP file transfers are restricted to the /var/home/ftp/pub directory. Permission for anonymous FTP users to create files in other directories is denied. You must enable the S8300 FTP server from

the Maintenance web page. The S8300 FTP server disables itself after 15 minutes.

3. Download the firmware files to the FTP or TFTP server.

   See Downloading Branch Gateway firmware files to a local TFTP server on page 118 or Installing firmware from the TFTP server on the S8300 Server on page 120.

4. Connect to the Branch Gateway via modem or via the Console port on the front panel.

   For information about connecting and enabling a modem for remote access, see Modems for remote access on page 61.

5. Run CLI commands.

   See CLI commands for upgrading Branch Gateway firmware via FTP/TFTP on page 115.

Related topics:

CLI commands for upgrading Branch Gateway firmware via FTP/TFTP on page 115
Example upgrade via FTP/TFTP using the CLI on page 116
CLI commands for upgrading Branch Gateway firmware via SCP on page 116
Installation worksheets on page 117
TFTP server setup on page 118
Downloading Branch Gateway firmware files to a local TFTP server on page 118
Installing firmware from the TFTP server on the S8300 Server on page 120

CLI commands for upgrading Branch Gateway firmware via FTP/TFTP

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 FTP or TFTP host as parameters. You must use the specific path to the file on the FTP or TFTP server according to the home directory of the service (FTP or TFTP) that you are using. When you enter the command, the CLI prompts you for a username and password.

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

- Use the **copy tftp module** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from a TFTP server
- Use the **copy tftp SW_imageA** command to upgrade the 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

Example upgrade via FTP/TFTP using the CLI

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

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

Note:

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

Note:

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

The following example uploads a firmware version with the path and file name *C:\g*xxx*.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:\gXXX.net 149.49.134.153
```

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 EW_archive** command to upgrade the Java applet for Avaya Branch Gateway Manager software from an SCPserver
- 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

Installation worksheets

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

Related topics:

Server Values worksheet on page 117
TFTP Server worksheet on page 118

Server Values worksheet

Table 10: 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	
Branch Gateway Device Manager	
MM710 E1/T1 media module	
MM710B E1/T1 media module	
MM711 Analog Port/Trunk media module	
MM712 DCP media module	
MM714 Analog Port/Trunk media module	
MM714B Analog Port/Trunk media module	
MM716 Analog Port/Trunk media module	
MM717 24-port DCP media module	
MM720 BRI media module	
MM721 BRI media module	
MM722 BRI Trunk media module	

TFTP Server worksheet

Table 11: Global Settings for TFTP Server

TFTP Server IP Address	TFTP Server Directory

TFTP server setup

To load single firmware files on an Branch Gateway, you must put the files on a computer connected to the customer's LAN or on an S8300 Server in the customer's network. You log on to the Branch Gateway later and use the gateway's TFTP capability to download the new firmware. If you can use an S8300 Server to stage the firmware, see Installing firmware from the TFTP server on the S8300 Server on page 120. If not, you must set up a TFTP server on the LAN.

Note:

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

Downloading Branch Gateway firmware files to a local TFTP server

Procedure

1. Access the www.avaya.com/support website.
2. Navigate to Media Gateway downloads.
3. Locate the file names that match the files listed in your installation worksheet.
   See Sample software and firmware filenames on page 119 for sample firmware file names.
4. Double-click the file name of the file you want to download.
   A File Download window appears.

   Note:

   Downloading files can occasionally add a [1] to the file name. Rename the file if necessary.
5. Select **Save this file to disk**.

6. Save the file to directory on the TFTP server on the local LAN that was created for this purpose.

   See Setting up a TFTP server on page 118.

Result

Note:

If you are performing the upgrade using the Branch Gateway's Command Line Interface (CLI), you can place the upgrade files on an FTP server.

Related topics:

Sample software and firmware filenames (continued) on page 119

Sample software and firmware filenames (continued)

Component	File name Example
Branch Gateway Processors	
Branch Gateway Processor	*gxxx_sw_21_11_0.bin*
Branch Gateway Device Manager	*gxxx_emweb_1_0_7.bin*
media modules	
MM710 E1/T1 media module	*mm710v3.fdl*
MM710B E1/T1 media module	*mm710v3.fdl* *mm710bv47.fdl*
MM711 Analog Port/Trunk media module (version 6 or earlier)	*mm711v16.fdl*
MM711 Analog Port/Trunk media module (version 7)	*mm711h7v21.fdl*
MM711 Analog Port/Trunk media module (version 20 or later)	*mm711h20v54.fdl*
MM712 DCP media module	*mm712v14.fdl*
MM714 Analog Port/Trunk media module	*mm714v5.fdl*
MM714B Analog Port/Trunk media module	*mm714h10v93.fdl*
MM716 Analog Port/Trunk media module	*mm716v80.fdl*
MM717 DCP media module	*mm717v3.fdl*
MM720 BRI media module	*mm720v1.fdl*
MM721 BRI media module	*mm721v1.fdl*
MM722 BRI media module	*mm722v3.fdl*

Installing firmware from the TFTP server on the S8300 Server

About this task

Instead of using a separately configured TFTP server on the LAN, you can use the TFTP server capability of an S8300 Server to stage the firmware for upgrading the Branch Gateway.

Note:

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

Procedure

1. Copy the individual firmware files to the */var/home/ftp/pub directory* on the S8300 Server using the Download Files web page on the S8300 Server.
2. Copy the files to the */tftpboot* directory of the S8300 Server.
3. After copying the files to the */tftpboot* directory, you can use the GIW to install the files to the Branch Gateway or its media modules by specifying the S8300 Server's IP address as the TFTP server containing the new firmware files.

Related topics:

Copying firmware files to the /tftpboot directory of an S8300 Server on page 120

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

Procedure

1. Use ssh craft@<ip address> to access the S8300 Server command line.
2. Address the password/challenge as required for access.
3. At the Linux prompt, type **cd /var/home/ftp/pub** and press Enter.

   The Linux prompt reappears. The current directory has changed to */var/home/ftp/pub*.
4. At the Linux prompt, type **mv <firmware_filename> /tftpboot**, and press Enter to move the firmware file to the */tftpboot* directory.

   To move multiple firmware files (most firmware files have an .bin suffix; the media module firmware files have a .fdl suffix), use the command **mv *.bin /tftpboot** or **mv *.fdl /tftpboot**. The Linux prompt reappears. The firmware file has been moved to the */tftpboot* directory. If you copy the firmware using the cp command, remove the files from the */var/home/ftp/pub* directory after you have copied them.

5. Repeat step 4 on page 0 , if necessary, for each firmware file you want to install.
6. At the Linux prompt, type **cd /tftpboot**.

   The Linux prompt reappears. The current directory has changed to */tftpboot*.
7. At the Linux prompt, type **ls**, and press Enter.

   A list of files in the directory appears.
8. Check the directory to make sure the firmware files you want to install are listed.

Upgrading 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 117.
2. Download the firmware files to a PC.

   See Downloading Branch Gateway firmware files to a local PC on page 122.
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 122.

Related topics:

CLI commands for upgrading Branch Gateway firmware via a USB device on page 122
Example upgrade using the CLI via a USB device on page 122
Downloading firmware files to a local PC on page 122

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 EW_archive`** command to upgrade the Java applet for Avaya Gxxx Manager software from a USB mass storage device
- Use the **`copy usb module`** command, followed by the slot number of the module you want to upgrade, to upgrade the firmware on a media module from a USB mass storage device
- Use the **`copy usb SW_imageA`** command to upgrade the 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 usb-device0 \temp\mm712v51.fdl 3
```

Downloading firmware files to a local PC

Procedure

1. Access the www.avaya.com/support website.
2. Navigate to Media Gateway downloads.
3. Locate the file names that match the files listed in your installation worksheet.

   See Sample software and firmware filenames on page 119 for sample firmware file names.
4. Double-click the file name of the file you want to download.

   A File Download window appears.
5. Select **Save this file to disk**.
6. Save the file to a directory on the local PC.

Result

Note:

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

Chapter 11: Upgrading IP phone configuration and firmware files

IP phone configuration and firmware file upgrades

The 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 its outgoing directory for phone images and scripts.

Note:

TFTP server support is only available on IPv4.

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

Note:

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

IP telephones supported by the local TFTP Server feature

- H.323:
  - 4601
  - 4601+
  - 4602
  - 4602SW
  - 4602SW+
  - 4606

- 4610SW
- 4612/24
- 4620
- 4620SW
- 4621SW
- 4622SW
- 4690

• SIP:

- 4602 SIP
- 4602SW
- 4602SW+
- 4610SW
- 4620SW
- 4621SW

IP telephones not supported by the local TFTP Server feature

• 4630

• 4630SW

Note:

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

Note:

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

Note:

The IP address of the TFTP server is the PMI.

Administering the upgrade

When using supported IP phones with the 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 topics:

Upgrading the IP telephone on page 127

Upgrading the IP telephone

About this task

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:

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

Note:

The 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 Administration for the Avaya G450 Branch Gateway, 03-602055

Procedure

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 129, otherwise proceed to step 6 on page 0 .

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.

Result

Note:

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

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 topics:

Upgrading the 4602SW and 4602D phones on page 129
Upgrading 4620 IP phones on page 131

Upgrading the 4602SW and 4602D phones

1. Check the available memory size for the image files using the **show application-memory** command. If the memory size is smaller than the

combined sizes of the image files for the phones, proceed to step 2 on page 130, otherwise proceed to step 5 on page 130.

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 telephone using the **copy ftp phone-image** command. For example:

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

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

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

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

```
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.

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
```

Result

Note:

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

Failure scenarios and repair actions

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

Table 12: 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	You tried to download configuration files after configuring the total memory	None. The memory allocations are set to the default values.

Problem	Possible cause	Action
server application memory sizes restore to defaults”	allocations for applications and Sniffer to more than 12 Mb in the startup configuration and performing a reset.	
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.
“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.

Upgrade 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 Branch Gateway.

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

Chapter 12: Backing up and restoring the Branch Gateway

Branch Gateway backups and restores

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

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

For information about Branch Gateway backup and restore, see *Administration for the Branch Gateway*.

Chapter 13: Troubleshooting

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.

Related topics:

[One telephone stops working](#) on page 137
[No power on the Branch Gateway](#) on page 138
[CLI is not accessible](#) on page 138
[NVRAM Init](#) on page 138

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.

Related topics:

[Identifying the problem when one phone stops working](#) on page 137

Identifying the problem when one phone stops working

Proposed Solution

Procedure

1. Replace the telephone.

   If the new telephone works, the problem is with the telephone itself. If the new telephone does not work, go on to the next step.

2. See *Maintenance Procedures for Communication Manager, Media Gateways and Servers*, 03-300432 for further information.

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 Appendix A: Front panel description on page 143.

CLI is not accessible

Check the connectivity to the Branch Gateway: correct 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 main board.

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 1

Procedure

1. Remove the Branch Gateway main board as described in Removing and inserting the Branch Gateway main board on page 90.
2. To determine the G450 main board version number, look for the label on the main board. The label includes the CS number. The number following “CS” is the main board version number.

   Version 1.x differs from version 2.x and 3.x in the placement of components on the main board.
3. Locate the NVRAM init jumper towards the front of the Branch Gateway main board.
   a. In Branch Gateway 1.x, the jumper is labeled *P5* .
   b. In Branch Gateway 2.x and 3.x, the jumper is labeled *NVRM_INIT*.

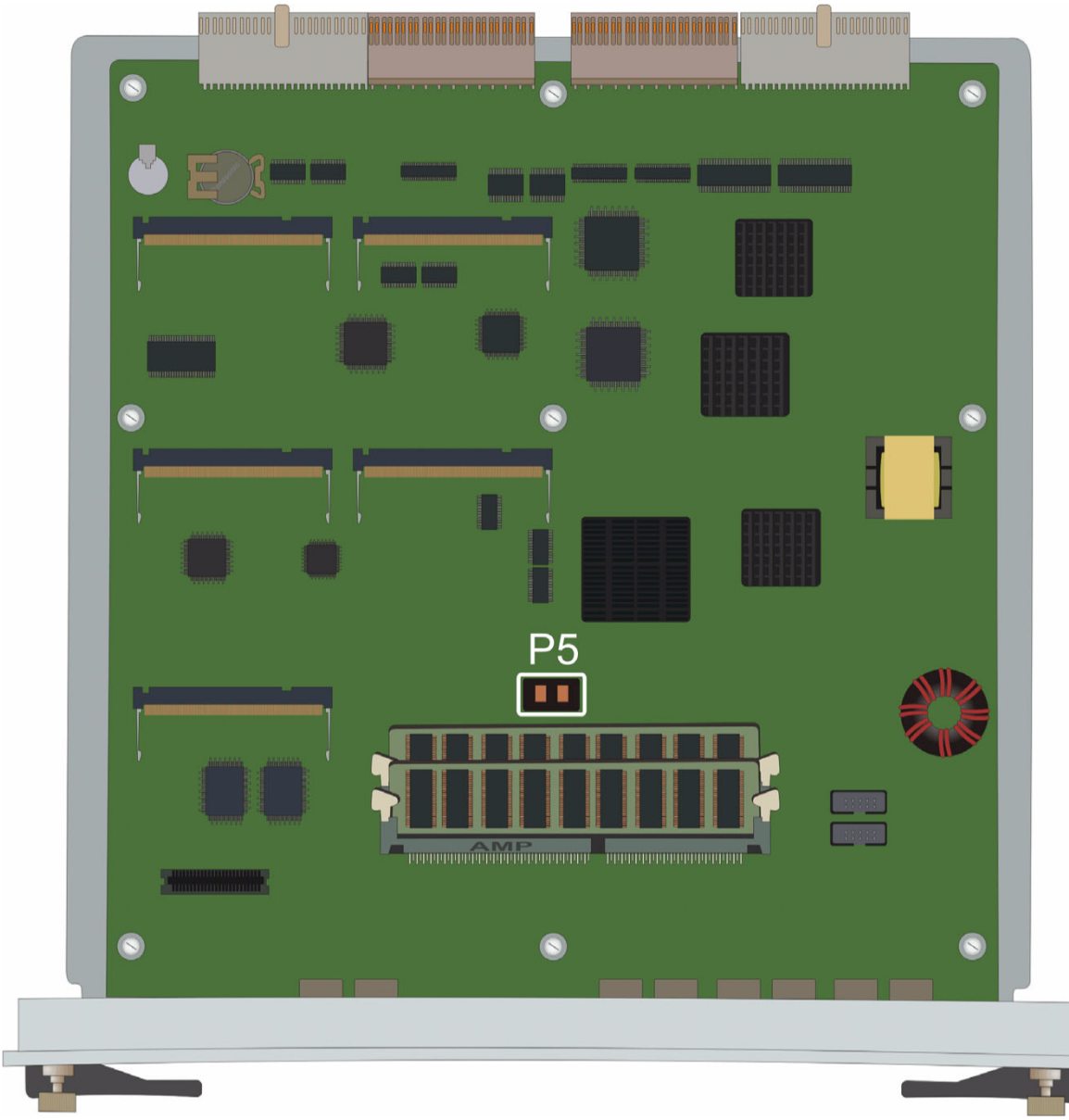


Figure 37: NVRAM INIT Jumper in the G450 Branch Gateway 1.x

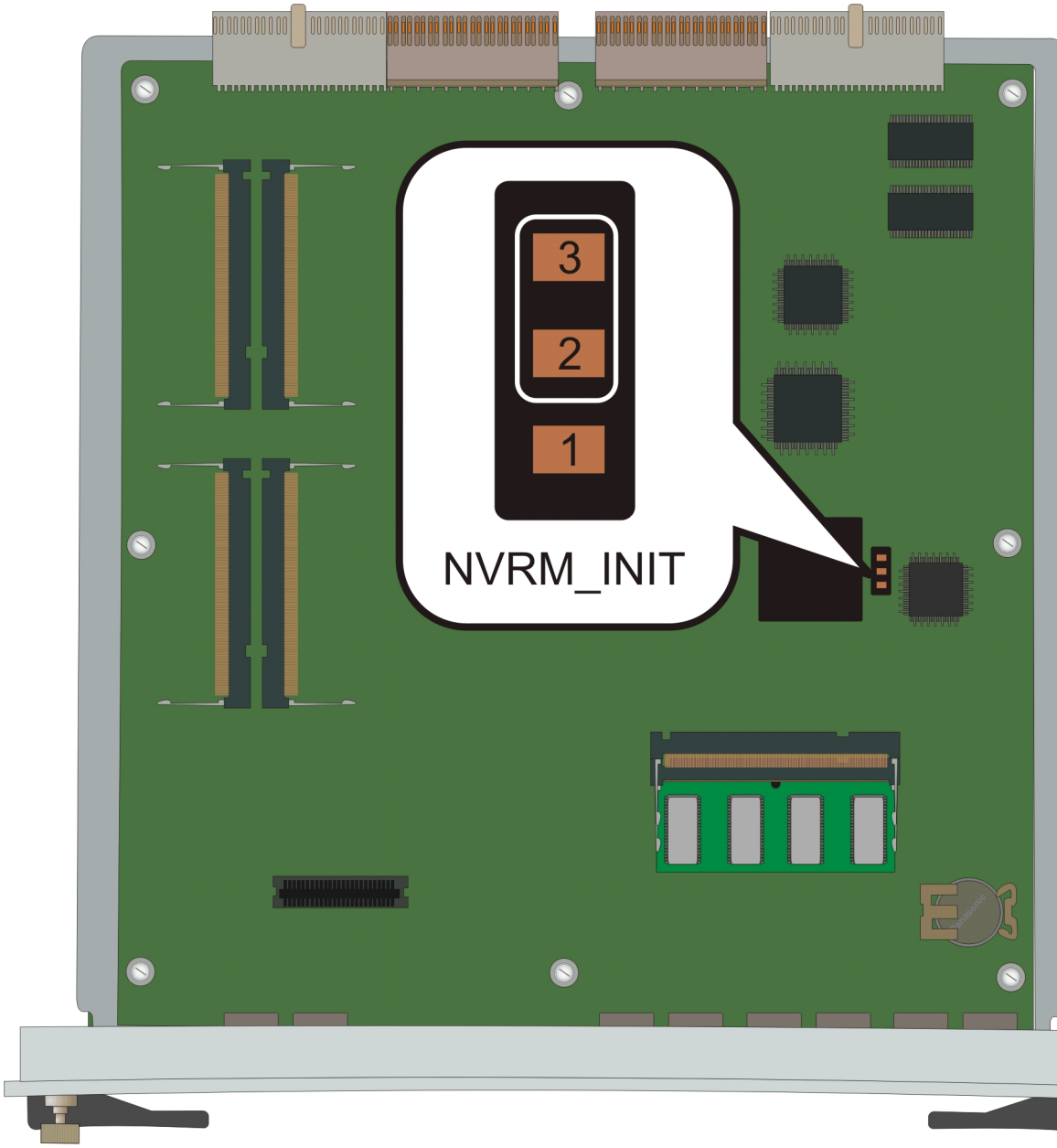


Figure 38: NVRAM INIT Jumper in G450 Branch Gateway 2.x and 3.x

4. Bridge the NVRAM INIT jumper:
   a. In a G450 Branch Gateway 1.x, use the bridge provided in the accessory kit to bridge jumper P5.
   b. In a G450 Branch Gateway 2.x and 3.x, use the bridge provided in the accessory kit to bridge pins 2 and 3 of the NVRM INIT jumper.

      Pins 2 and 3 are closer to the front panel of the main board.
5. Insert the Branch Gateway main board as described in Removing and inserting the Branch Gateway main board on page 90.

6. Let the Branch Gateway operate for about 5 minutes so that it will boot and erase the current configuration.
7. Remove the Branch Gateway main board as described in Removing and inserting the Branch Gateway main board on page 90.
8. Remove the bridge.

   Important:

   If you do not remove the bridge, the Branch Gateway will continue to initialize the NVRAM when it resets or is powered up.
9. Insert the Branch Gateway main board as described in Removing and inserting the Branch Gateway main board on page 90.

Chapter 14: Front panel description

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

Related topics:

The front panel of the Branch Gateway chassis without media modules on page 143
The front panel of the Avaya MM340 media module on page 149
The front panel of the Avaya MM342 media module on page 150
The front panel of the Avaya MM710B media module on page 151
The front panel of the Avaya MM711 media module on page 152
The front panel of the Avaya MM712 media module on page 153
The front panel of the Avaya MM714 media module on page 154
The front panel of the Avaya MM714B media module on page 155
The front panel of the Avaya MM716 media module on page 156
The front panel of the Avaya MM717 media module on page 158
The front panel of the Avaya MM720 media module on page 160
Front panel of the MM721 media module on page 161
The front panel of the Avaya MM722 media module on page 162

The front panel of the Branch Gateway chassis without media modules

There are two hardware versions of the G450 Branch Gateway, referred to as *G450 Branch Gateway 1.x* and *G450 Branch Gateway 2.x*. 1.x and 2.x refer to the hardware suffix of the Branch Gateway that is printed on the label displayed on the rear of the chassis. The

differences between the two versions are minor, and include slightly different front panels, and different placement of components on the main boards.

- On the G450 version 1.x, the RST button is to the *left* of the ASB button.
- On the G450 version 2.x, the RST button is *above* the ASB button.

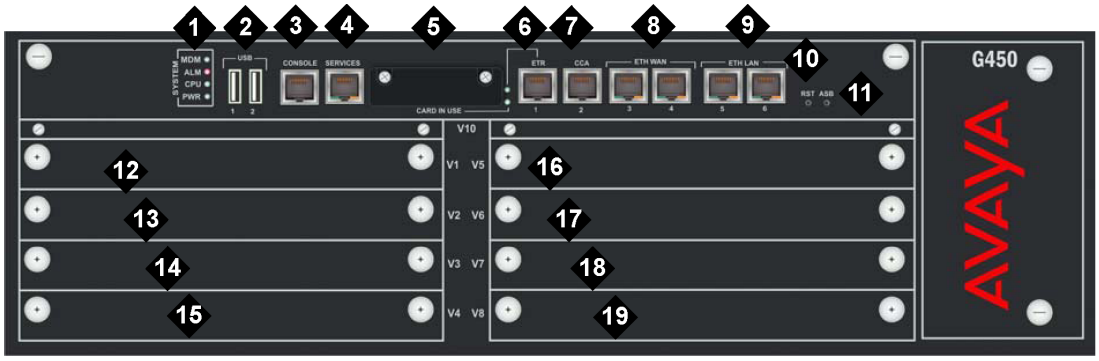


Figure 39: The G450 1.x front panel ports and slots

Figure 40: The G450 2.x front panel ports and slots

Related topics:

[Media module slots](#) on page 145
[System LEDs](#) on page 145
[USB ports](#) on page 145
[Console port (Console)](#) on page 145
[Services port (Services)](#) on page 146
[Compact Flash Interface](#) on page 146
[The Emergency Transfer Relay port](#) on page 146
[Contact Closure port](#) on page 147
[Router ports (ETH WAN)](#) on page 147
[Switch ports (ETH LAN)](#) on page 148
[RST and ASB buttons](#) on page 148

Media module slots

The G450 has eight standard media module slots (V1 through 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 allocations on page 31.

System LEDs

Table 13: System LEDs

LED	Name	Color	Indication
MDM	Modem Detected	Green	A modem is connected to the CONSOLE or 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

USB ports

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

- USB flash drive
- USB modem. See USB modems supported by the Media Gateway on page 164 for a list of supported USB modems.

Console port (Console)

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 a cross-over Ethernet cable.

Services port (Services)

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

Note:

Use a cross-over Ethernet cable.

Compact Flash Interface

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

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

Table 14: Compact Flash CARD IS USE LED states

LED	State	Meaning
CARD IN USE	Steady yellow	A compact flash card is inserted but not being used. You can safely remove the card. (G450 1.x only).
	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 you can remove the compact flash card (G450 2.x only).

The Emergency Transfer Relay 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 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 58.

Related topics:

Implementing the Contact Closure feature on page 147

Implementing the Contact Closure feature

About this task

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

Router ports (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.

Each ETH WAN port 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. 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.

Related topics:

Loading firmware from a bank other than the default bank during startup on page 148

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 MM340 media module

The MM340 media module provides one WAN access port for the connection of an E1 or T1 WAN line.

Figure 41: The MM340 media module front panel

Related topics:

MM340 ports on page 149
MM340 LEDs on page 149

MM340 ports

The MM340's E1/T1 WAN access port is marked E1/T1. This port is located in the center of the front panel.

MM340 LEDs

Table 15: MM340 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	A port is being initialized or a loopback is present
ACT	Activity	Yellow	At least one PPP/Frame Relay session is active
SIG	Signal	Green	The physical connection is up.

The front panel of the Avaya MM342 media module

The MM342 media module provides one USP WAN access port and supports the following WAN interface types:

- V.35/ RS449
- X.21

Figure 42: The MM342 media module front panel

Related topics:

MM342 ports on page 150
MM342 LEDs on page 150

MM342 ports

The MM342 contains one WAN SCSI access port.

MM342 LEDs

Table 16: MM342 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	A port is being initialized or a loopback is present
ACT	Activity	Yellow	At least one PPP/Frame Relay session is active
CON	Connection	Green	The physical connection is up

The front panel of the Avaya MM710B media module

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

Note:

This information also applies to the MM710.

Note:

For drop and insert, an external CSU is required.

Figure 43: The MM710B media module front panel

Note:

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

Related topics:

MM710B ports on page 151
MM710B LEDs on page 151

MM710B ports

The MM710B contains an E1/T1 port.

MM710B LEDs

Table 17: 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

LED	Name	Color	Indication
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.

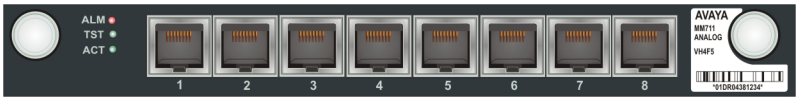


Figure 44: The MM711 media module front panel

Related topics:

MM711 ports on page 152
MM711 LEDs on page 153

MM711 ports

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

MM711 LEDs

Table 18: 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 45: The MM712 media module front panel

Related topics:

MM712 ports on page 153
MM712 LEDs on page 154

MM712 ports

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

MM712 LEDs

Table 19: 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 46: The MM714 media module front panel

Related topics:

MM714 ports on page 154
MM714 LEDs on page 155

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 20: MM714 LEDs

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

The front panel of the Avaya MM714B media module

The MM714B analog media module provides all the features provided by the MM714 (see The front panel of the Avaya MM714 media module on page 154), 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 47: The MM714B media module front panel

Related topics:

MM714B ports on page 155
MM714B LEDs on page 156

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 21: 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 **`set etr manual-on`** 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 48: The MM716 media module front panel

Related topics:

MM716 ports on page 157

MM716 LEDs on page 158

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 22: 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

Station port	Cable pair	
24	Violet	Brown
OPEN	Violet	Slate

MM716 LEDs

Table 23: 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 49: The MM717 media module front panel

Related topics:

MM717 ports on page 158
MM717 LEDs on page 160

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 24: 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 25: 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 50: The MM720 media module front panel

Related topics:

MM720 ports on page 160
MM720 LEDs on page 160

MM720 ports

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

MM720 LEDs

Table 26: MM720 LEDs

LED	Name	Color	Indication
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot

LED	Name	Color	Indication
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

Related topics:

MM721 media module ports on page 161
MM721 media module LEDs on page 161

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.

LED	Name	Color	Indication
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 51: The MM722 media module front panel

Related topics:

MM722 ports on page 162
MM722 LEDs on page 162

MM722 ports

The MM722 contains two ISDN BRI ports.

MM722 LEDs

Table 27: 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

Technical specifications

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

Related topics:

Specifications on page 163
Power cord specifications on page 164
USB modems supported by the Branch Gateway on page 164
USB modems supported by the S8300 on page 164

Specifications

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

Table 28: Avaya Branch Gateway G450 specifications

Description	Value
Height	5.25 in. (3U, 133.3 mm)
Width	19 in. (482.6 mm)
Depth	18 in. (460 mm)
Weight of empty chassis	16.5 pounds (7.5 kg)
Weight of chassis with basic configuration, including main board, power supply unit, fan tray, one DSP, and blank panels on the media module slots	31 pounds (14 kg)
Ambient working temperature	32° to 104°F (0° to 40°C)
Storage temperature	–40°F to 150°F (–40°C to 66°C)
Operation altitude	up to 10,000 ft. (3000 m)
Front Clearance	12 in. (30 cm)

Description	Value
Rear Clearance	18 in. (45 cm)
Humidity	10 to 90% relative humidity, non-condensing
Power rating	90-264 VAC, 47-63 Hz
BTU	1,780 BTU/h
Max current	7 A

Power cord specifications

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

For North America:

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

For Outside North America:

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

USB modems supported by the 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

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 169
- Call Center on page 169

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.

Related topics:

Typical adjunct power connections on page 167
Typical adjunct power connections end-to-end on page 168
Avaya Aura Communication Manager messaging application on page 169
Call Center on page 169

Typical adjunct power connections

The 400B2 adapter is convenient for connecting local -48 VDC power to a modular plug. See the figure on page 168.

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

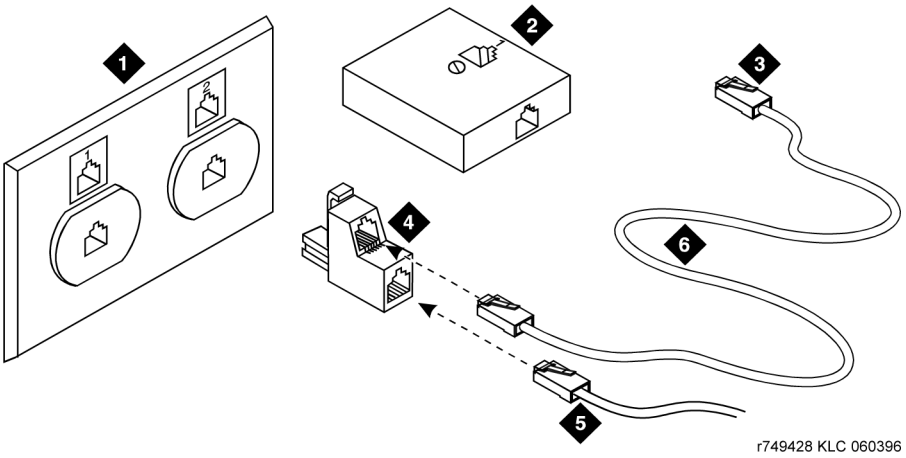


Figure 52: 400B2 Adapter Connecting to a Modular Plug

Table 29: 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.

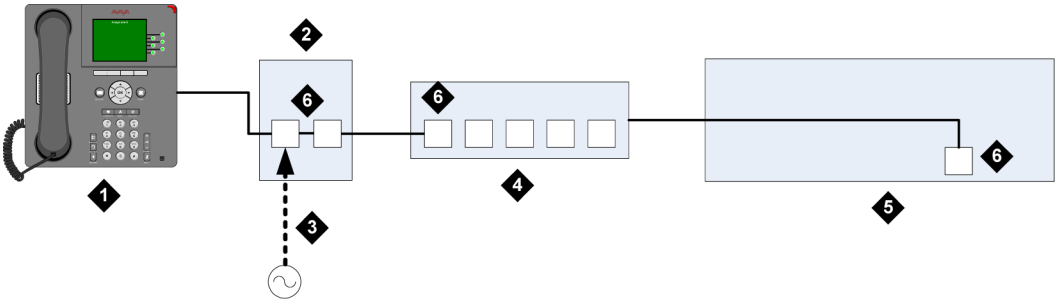


Figure 53: Example Adjunct Power Connections

Table 30: 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 touchtones, converts messages to the G.711 format, and converts text to speech.

Call Center

The S8300 Server provides an excellent solution for a small Call Center. The S8300 Server with one or more Branch Gateways supports the following Call Center capabilities:

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

Related topics:

About Avaya Branch Gateway announcement software on page 169

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* and configure the G450 in the media-gateway form.

Chapter 17: Information checklists

Information checklists

You can use the 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 171: Tools, software, laptop settings, customer network information
- Serial number and login information: Serial number of the Branch Gateway and login/ passwords for various access methods
- Quick setup for Media Gateway Processor (MGP) on page 173: IP addresses and setup commands for the MGP
- Installation site information on page 174: Customer and site contact information

Related topics:

Installer's checklist on page 171

Installer's checklist

	Tools
	laptop with 32 MB RAM
	40 MB available disk space
	RS-232 port connector or Ethernet interface
	cross-over Ethernet cables
	direct Ethernet cable
	USB flash drive (optional)
	screwdriver
	Software
	Windows 95/98/ME/XP/NT/2000/Vista operating system

	FTP server program. TFTP server program and SCP server program are recommended
	SSH program
	terminal emulation program: HyperTerminal or other
	TCP/IP networking software: bundled with Windows OS
	web browser: Netscape 4.7x or Internet Explorer 5.0
	Ethernet connections
	laptop default address and mask: 192.11.13.5, 255.255.255.252
	browser: no proxies
	communications properties: 9600 baud rate; no parity; 8 data bits, 1 stop bit; no flow control
	SSO login
	Obtaining this login will require that you complete the authentication process. You will not be able to obtain the license file or to perform remote feature activation without the SSO login authentication process. You will not be able to obtain the license file or to perform remote feature activation without the SSO login.
	Dial plan
	IP addressing plan
	List of customer-provided IP services

Serial number and login information

Branch Gateway serial number

Logins

	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**	
	In the context of the interface, assign an IP address and subnet mask to the interface: **ip address**	**IP address**	
		netmask	
	In the context of the interface, define this interface as the PMI **pmi**		
Configure the ICC-VLAN **Note:** By default, the ICC-VLAN is 1. Therefore configure the ICC-VLAN only if you wish to configure it for a VLAN other than 1.	Create a vlan and enter its configuration context: **interface vlan**	**vlan id**	
	In the context of the vlan interface, set the current vlan as the icc-vlan: **icc-vlan**		
	Set the VLAN ID of a LAN port (10/5 or 10/6) to the VLAN number of the ICC-VLAN: **set port vlan**	**vlan id**	
		module number	
		port number	
Define the CLI prompt	**hostname**	**hostname**	

Define a default gateway	**ip default-gateway**	**gateway IP address**	
Create a list of valid Media Gateway Controller(s)	**set mgc list**	**IP address1**	
		IP address2	
		IP address3	
		IP address4	
Display device information	**show system**		

Installation site information

Site Name	Main Phone
Installation Address	
Shipping Address	
Customer Contact	Name: Title: Phone: Fax: Mobile: Pager: 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

Equipment list

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

Note:

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

Table 31: Equipment List: G450 Branch Gateway

The G450 Branch Gateway is a 19-inch 3Uu 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/gatekeeper. It also houses eight 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.		
Material Code:170896	Apparatus Code: MGW1	Not Optional
Branch Gateway Comcodes (for Services Ordering Only)		
Comcode	Number of Items	Description
700407802	1	Branch Gateway chassis/Main board/80 channel DSP daughterboard/ 1 PSU
700432487	1	Branch Gateway chassis/Main board/20 channel DSP daughterboard/ 1 PSU
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)
700439011	1	Branch Gateway PSU Blank Panel
700179526	1	Documentation, CIB 3246 FCC/ Safety Branch Gateway
700236680	1	Grounding Kit for multiple Branch Gateways in a 19 inch rack
700439029	1	Cable grounding terminal-ring to open end 10AWG, 8M
Branch Gateway Comcodes for Customer and Services ordering		
Comcode		Description
700407802		Branch Gateway chassis/Main board/80 channel DSP daughterboard/ 1 PSU
700432487		Branch Gateway chassis/Main board/20 channel DSP daughterboard/ 1 PSU
700432495• 700504684		Branch Gateway main boardG450 Main Supervisor Board Re-Designed Non-GSA
700432503		80 channels DSP daughterboard
700432511		20 channels DSP daughterboard
700432529		Branch Gateway Power Supply Unit 400W AC
700432537		Branch Gateway Chassis
700438278		Branch Gateway Fan tray
700394992		808A Emergency Transfer Panel
700457013		Upgrade memory kit

Table 32: Equipment List: EM200 Expansion Module

EM200 Expansion Module
The EM200 Expansion Module is a 19-inch 1.5U rack-mountable device. The EM200 houses two Media Module Bays, and serves as an extension to the Branch Gateway. You can connect up to two EM200 modules to an Branch Gateway.
EM200 Comcodes (for Services Ordering Only)

EM200 Expansion Module		
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 EM200s in a 19 inch rack

Table 33: Equipment List: Branch Gateway Power Cords

Branch Gateway Power Cords		
Supplies Power to the Branch Gateway. One cord per gateway is required, and there are various cords depending on the power required for the country in which the unit will be installed.		
Material Code: 170904	Apparatus Code: none	Not Optional
When you order this material code, a descriptive attribute will be required; the attributes are:		
Attribute	Option	Comcode: Description
CRD	30	405362641: PWR CORD 9X10IN USA 17505
CRD	31	407786623: PWR CORD 98IN EUROPE 12013S
CRD	32	407786599: PWR CORD 98IN UNITED KINGDOM 14012
CRD	33	407786631: PWR CORD 98IN AUSTRALIA 15012
CRD	34	407790591: PWR CORD INDIA P250CIM
CRD	42	408161453: PWR CORD 96IN ARGENTINA

Table 34: Equipment List: Avaya S8300C Server

Server
S8300C Server
The Avaya S8300C Server is an Intel™-based server complex that carries: • Administration and maintenance provisioning software • Hard drive (Field-replaceable. Comcode: 700307028) • One GB RAM • Web serve • Linux OS • H.248 Branch Gateway Signaling Protocol • CCMS messages tunneled over H.248 Signaling Protocol • TFTP server The S8300D Server can act as the primary server of the Branch Gateway, or it can serve as a local survivable processor for remote/branch customer locations.
Comcode (for Services Ordering Only): 700407810

Table 35: Equipment List: Media Modules

Media Modules	
MM710 T1/E1 Media Module	Comcodes (for Services Ordering Only): 700394737, 700439250, 700466634
The MM710 T1/E1 media module offers the combined features of a DEFINITY DS1 circuit pack and includes the following: • A built-in CSU • AMI-BASIC • Both A-law for E1 and μ -law for T1 • Line Coding: AMI, ZCS, B8ZS for T1 and HDB3 or AMI for E1 • Stratum 3 Clock compatibility • Trunk signaling for supporting US and International CO trunks and tie trunks as currently in existence The MM710 T1/E1 media module supports the universal DS1 conforming to 1.544 Mbps T1 standard and 2.048 Mbps E1 standard. ISDN PRI is also supported for T1 or E1 revenue-associated option. The MM710 is RoHS compliant.	
MM710B T1/E1 Media Module	Comcodes (for Services Ordering Only): 700394737, 700439250, 700466634

Media Modules
The MM710B T1/E1 media module offers the combined features of a DEFINITY DS1 circuit pack and includes the following: • A built-in CSU • AMI-BASIC • Both A-law for E1 and μ -law for T1 • Line Coding: AMI, ZCS, B8ZS for T1 and HDB3 or AMI for E1 • Stratum 3 Clock compatibility • Trunk signaling for supporting US and International CO trunks and tie trunks as currently in existence The MM710B T1/E1 media module supports the universal DS1 conforming to 1.544 Mbps T1 standard and 2.048 Mbps E1 standard. ISDN PRI is also supported for T1 or E1 revenue-associated option. The MM710B is RoHS compliant.

DEF DS1 LOOPBACK JACK 700A		
Provides the ability to remotely troubleshoot the MM 710 T1/E1 media module. It is required for any customer with a maintenance contract and highly recommended for any other customer.		
Material Code: 700406101	Apparatus Code: None	Required for any customer with a maintenance contract and an MM710 or MM7110B T1/E1 media module. Highly recommended for other customers to avoid expensive technician visits.

MM711 Analog Media Module	Comcodes (for Services Ordering Only): 700394661, 700466626
The MM711 Analog media module supports eight analog interfaces allowing the connectivity of Loop Start, Ground Start, Analog DID trunks, and 2-wire analog Outgoing CAMA E911 trunks. The MM711 Analog media module also allows connectivity of analog, tip/ring devices such as single line telephones, modems or group 3 fax machines. Each port may be configured as either a trunk interface or a station interface. Also included is support for caller ID signaling, ring voltage generation for a variety of international frequencies and cadences, and administrable line termination styles. The MM711 is RoHS compliant.	

MM714 Analog Media Module	Comcode (for Services Ordering Only): 700395221
The MM714 Analog media module supports four analog stations and four CO trunks. Analog DID trunk connections are to be associated with the ports labeled “Line” and not “Trunk”. The MM714 is RoHS compliant.	

Media Modules	
MM714B Analog Media Module	Comcodes (for Services Ordering Only): 700453889, 700466618
The MM714B Analog media module supports four analog stations and four CO trunks, as well as an Emergency Transfer Relay between a line port and a trunk port. Analog DID trunk connections are to be associated with the ports labeled “Line” and not “Trunk”. The MM714B is RoHS compliant.	
MM712 DCP Media Module	Comcode (for Services Ordering Only): 700394745
The MM712 DCP media module allows connectivity of up to eight 2-wire DCP voice terminals. MM712 does not support 4-wire DCP telephones. Signal timing specifications for the MM712 support TDM Bus Timing in receive and transmit modes. The Branch Gateway supplies only +5 VDC and –48 VDC to the MM712 media module. Any other required voltages must be derived on the module. Loop range secondary protection is provided on the MM712. The MM712 is also self-protecting from an over current condition on a tip and ring interface. The MM712 is RoHS compliant.	
MM716 24 port Analog Media Module	Comcodes (for Services Ordering Only): 700394703, 700466642
The MM716 provides 24 analog ports supporting telephones, modem, and fax. These ports can also be configured as DID trunks with either wink-start or immediate-start. The 24 ports are provided via a 25-pair RJ21X amphenol connector, which can be connected by an amphenol cable to a breakout box or punch down block. The MM716 is RoHS compliant.	
MM717 24 port DCP Media Module	Comcode (for Services Ordering Only): 700394711
The MM717 DCP Medial Module supports 24 DCP stations. The MM717 uses a 25-pair amphenol connector on the media module’s faceplate. The 24 DCP ports are intended for in-building use only. Phone lines connected to those ports are not to be routed out-of-building. Failure to comply with this restriction could cause harm to personnel or equipment. The MM717 is RoHS compliant.	
MM720 BRI Media Module	Comcode (for Services Ordering Only): 700394752
The MM720 BRI media module contains eight ports that can be administered either as BRI trunk connections or BRI endpoint (telephone and data module) connections. Information is communicated in two ways: • Over two 64 Kbps channels called B1 and B2 that can be circuit-switched simultaneously • Over a 16 Kbps channel called the D channel that is used for signaling. The D channel occupies one time slot for all eight D channels The circuit switched connections have a u-law or A-law option for voice operation. The circuit switched connections operate as 64 Kbps clear channels when in the data mode. The MM720 BRI media module does not support combining both B channels together to form a 128 Kbps channel.	

Media Modules

Note:

The MM720 BRI media module cannot be administered to support both BRI trunks and BRI endpoints at the same time.

For BRI trunking, the MM720 BRI media module supports up to eight BRI interfaces, or up to 16 trunk ports, to the central office at the ISDN S/T reference point.
For BRI endpoints, each of the eight ports on the MM720 BRI media module can support one integrated voice/data endpoint or up to two BRI stations and/or data modules. Supported endpoints must conform to AT&T BRI, World Class BRI, or National ISDN NI1/NI2 BRI standards. The MM720 BRI media module provides -40 volt phantom power to the BRI endpoints.
The MM720 is RoHS compliant.

MM721 BRI Media Module	Comcode (for Services Ordering Only): 700393762

The MM721 BRI media module contains eight ports that can be administered either as BRI trunk connections or BRI endpoint (telephone and data module) connections. Information is communicated in two ways:

- Over two 64 Kbps channels called B1 and B2 that can be circuit-switched simultaneously
- Over a 16 Kbps channel called the D channel that is used for signaling. The D channel occupies one time slot for all eight D channels

The circuit switched connections have a u-law or A-law option for voice operation. The circuit switched connections operate as 64 Kbps clear channels when in the data mode.
The MM720 BRI media module does not support combining both B channels together to form a 128 Kbps channel.

Note:

The MM720 BRI media module cannot be administered to support both BRI trunks and BRI endpoints at the same time.

For BRI trunking, the MM720 BRI media module supports up to eight BRI interfaces, or up to 16 trunk ports, to the central office at the ISDN S/T reference point.
For BRI endpoints, each of the eight ports on the MM720 BRI media module can support one integrated voice/data endpoint or up to two BRI stations and/or data modules. Supported endpoints must conform to AT&T BRI, World Class BRI, or National ISDN NI1/NI2 BRI standards. The MM720 BRI media module provides -40 volt phantom power to the BRI endpoints.
The MM720 is RoHS compliant.

MM722 2-port BRI Media Module	Comcode (for Services Ordering Only): 700395239

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

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W