Quick Start for Hardware Installation: Avaya G450 Branch Gateway

6.1
03-602053
Issue 7
February 2011

Notice

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

Warranty

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

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there 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 Fraud Intervention

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

Disclaimer

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

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

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.

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 TIATSB-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

CE

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

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 9
Site requirements on page 14

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 9
Obtaining the Branch Gateway serial number on page 10
RFA access on page 11
License file with Survivable Remote Server on page 11
Downloading license and authentication files on page 11
ART for the RAS IP address on page 12
Downloading recent firmware on page 14
The EPW on page 14

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 10
Equipment required for mounting on page 10
Equipment required for installing an S8300 Server on page 10

Equipment required if you are not installing an S8300 Server on page 10

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 for a list of the USB modems supported by the Branch Gateway).USB modems supported by the Branch Gateway

Obtaining the Branch Gateway serial number

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

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.

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 13

Obtaining the RAS IP address and password

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

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. 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 15
Verifying power outlets on page 15
Verifying the grounds on page 15

Verifying temperatures and clearances

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

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

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.

Warning:

Do not overload the power circuit.

Verifying the grounds

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

Warning:

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

Chapter 2: Unpack the device

Unpacking and checking package contents

For the Branch Gateway package:

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.

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.

Chapter 3: Mount the devices

Placing the Branch Gateway on a table

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

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.

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 20
Mounting the Branch Gateway on a wall on page 24

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 20
[Attaching a mounting bracket to the front of the Branch Gateway](#) on page 20
[Attaching a mounting bracket to the middle of the Branch Gateway](#) on page 21
[Brackets with cable guides](#) on page 21
[Attaching a mounting bracket with cable guides](#) on page 22
[Attaching each mounting bracket to the Branch Gateway](#) on page 22
[Before mounting the Branch Gateway](#) on page 23
[Mounting the Branch Gateway in the rack](#) on page 23

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

Attaching a mounting bracket to the middle of the Branch Gateway

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.

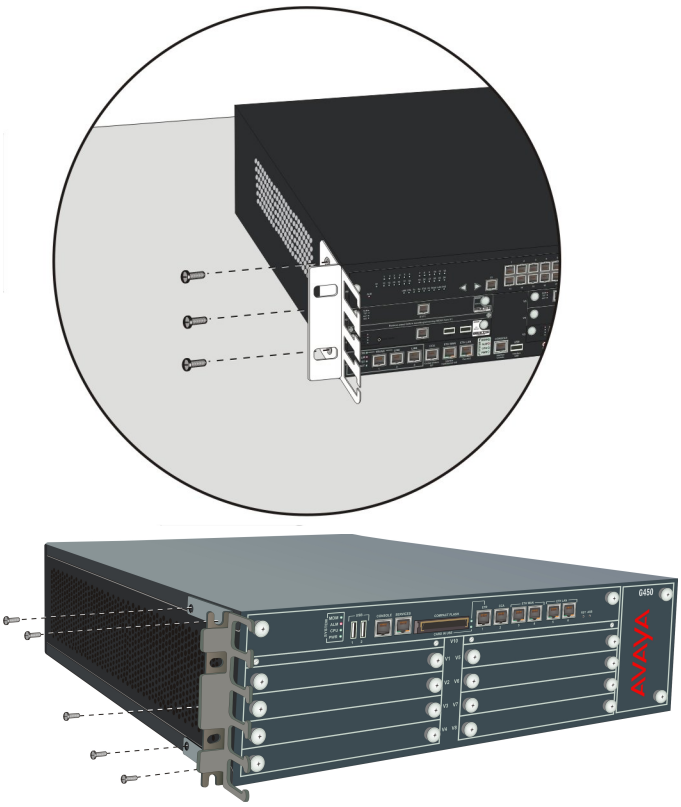
Note:

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.

Note:

Connecting a DCP telephone to an MM712 or MM717 media module

Attaching a mounting bracket with cable guides



Attaching each mounting bracket to the Branch Gateway

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.

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

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

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

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

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 21.

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 24
Fastening the Branch Gateway to the wall on page 25

Attaching brackets to the Branch Gateway for wall mounting

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

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

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

   Make sure the plywood is sufficiently anchored in the wall. Use a minimum of four wood screws and ensure the screws are driven into wall studs, or use four wall anchors rated not less than 50 pounds (22.5 kg) shear strength each.
2. Mark the plywood with the location of the 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).

Chapter 4: Install media modules

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 27
[Combination limitations](#) on page 28
[Slot allocation](#) on page 28
[Inserting the S8300 Server](#) on page 29
[Inserting media modules](#) on page 31

Before inserting media modules into the Branch Gateway chassis

- Do not install an unsupported combination of media modules. See [Combination limitations](#) on page 28.
- Allocate a permissible slot to each media module. See [Slot allocation](#) on page 28.

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 allocation

The Branch Gateway chassis has eight media module slots, marked V1, V2, V3, V4, V5, V6, V7, and V8 (see the figure 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.

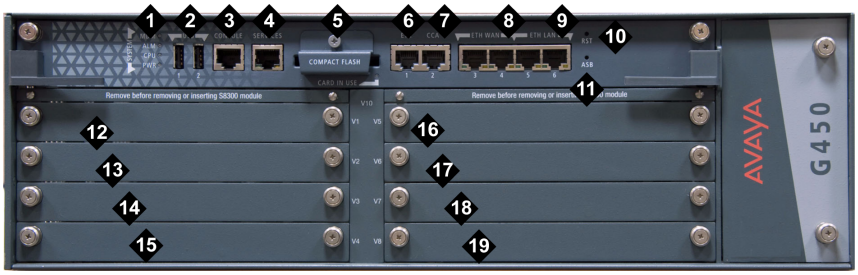


Figure 2: The G450 Branch Gateway front panel ports and slots

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

1. ASB button
2. V1 — slot for standard media module or S8300 Server
3. V2 — slot for standard media module
4. V3 — slot for standard media module
5. V4 — slot for standard media module
6. V5 — slot for standard media module
7. V6 — slot for standard media module
8. V7 — slot for standard media module
9. 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.
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.
MM721	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

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.

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 3: 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

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

Electrostatic alert:

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

Caution:

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

Caution:

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

1. Position the media module before the selected bay on the front of the 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.

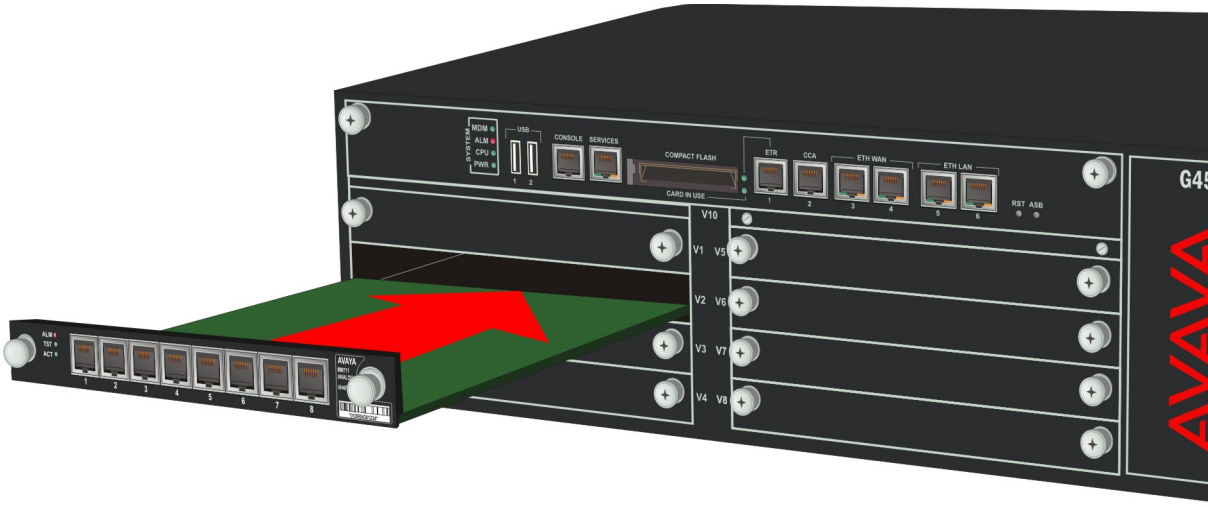


Figure 4: Inserting a media module

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.

Chapter 5: Power up

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.

Attaching the ground wires

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.

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.

Attaching ground wires for purchased ground blocks

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.

Connecting power to the Branch Gateway

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.

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 6: Prepare for configuration

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 . For detailed information on CLI commands, see the .

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 Chapter 4: Connecting and enabling a modem for remote access.
- Remotely through the network. For information about preparing a newly installed Branch Gateway for configuration via the network, see Configuring basic Branch Gateway connectivity on page 37.

Configuring basic Branch Gateway connectivity

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.

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.

Using the CLI

For information about configuring the G450 Branch Gateway with the Command Line Interface:

- For instructions on how to connect to the CLI, see Accessing the Avaya G450 Branch Gateway.
- For detailed information about CLI commands, see *Avaya Branch Gateway G450 CLI Reference*.

Index

E

F

G

I

L

M

P

R

S

T

U

V

W