Avaya G450 Branch Gateway Overview and Specification

Release 10.2.x
Issue 1
December 2023

Notice

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

Warranty

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Documentation disclaimer

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

Link disclaimer

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

Copyright

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

Virtualization

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

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Product Safety Standards

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

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

This product may contain Class 1 laser devices.

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

Electromagnetic Compatibility (EMC)

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

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

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

For a Class B digital device or peripheral:

Note:

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

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

Equipment With Direct Inward Dialing ("DID"):

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

Proper Answer Supervision is when:

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

Permissible exceptions are:

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

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

Automatic Dialers:

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

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

Toll Restriction and least Cost Routing Equipment:

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

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

For equipment approved prior to July 23, 2001:

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

For equipment approved after July 23, 2001:

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

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

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

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

Means of Connection:

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

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	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 LLC in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

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

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

Canadian Conformity Information

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

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

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

European Union Declarations of Conformity

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

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

European Union Battery Directive

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

Japan

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

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

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

If this is a Class A device:

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

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

If this is a Class B device:

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document provides a high-level understanding of Branch Gateway characteristics and capabilities, including interoperability, performance specifications, security, and licensing requirements. It is intended for system administrators, sales, and support personnel.

Chapter 2: Avaya G450 Branch Gateway overview

Avaya G450 Branch Gateway is a multifunctional gateway that you can deploy in medium to large-sized branch locations or wiring closets in servicing buildings.

G450 Branch Gateway provides the following functionality:

- Works in conjunction with Avaya Aura® Communication Manager IP telephony software.
- Combines phone exchange and data networking using PSTN toll bypass, routing data and VoIP traffic over a WAN.
- Provides a VoIP engine, an optional WAN router, and Ethernet LAN connectivity.
- Supports Avaya IP and digital phones, analog devices, such as modems, fax machines, and phones.

Phone services on a Branch Gateway are controlled by an Avaya or customer-provided server operating either as an External Call Controller (ECC) or as an Internal Call Controller (ICC). G450 Branch Gateway supports the Avaya S8300 Server as an ICC, or as an ECC when S8300 is installed on another Branch Gateway.

G450 Branch Gateway can support up to 450 users when deployed in a mid-to-large branch office of an enterprise or call center. This requires Avaya Aura® Communication Manager IP telephony software running on one or more Avaya servers. S8300 supports 50 Branch Gateways and other Avaya servers support up to 250 Branch Gateways.

G450 Branch Gateway hardware specifications

G450 Branch Gateway is a modular device with a basic configuration of one power supply unit. You can enhance this configuration by adding an additional PSU.

The following table describes G450 Branch Gateway hardware components in the basic and enhanced configuration.

G450 Branch Gateway hardware components	Basic configuration	Enhanced configuration
Number of Power Supply Units (PSUs)	1	2
RAM	256 MB / 1 GB in G450 v4	512 MB / 1 GB in G450 v4
DSP childboard	1 (160 VoIP channels)	Maximum 4 (up to 320 VoIP channels)
External compact flash	–	1024 announcement files

Minimum G450 Branch Gateway firmware requirements

Firmware version	Build	v1, v2	v3	Recommended Communication Manager version
BGW 10.2	43.9.0	Yes	Yes	AA 10.2, CM 10.2 AA 10.1.x, CM 10.1.x AA 10.1, CM 10.1 If your Branch Gateway is running Build 38.20.0 or earlier, you must install Release 7.1.0.4 Build 38.21.2 before upgrading to Build 43.9.0.
BGW 10.1.x	42.24.0	Yes	Yes	AA 10.1.x, CM10.1.x AA 10.1, CM 10.1 AA 8.1.x, CM 8.1.x AA 8.0.x, CM 8.0.x If your Branch Gateway is running Build 38.20.0 or earlier, you must install Release 7.1.0.4 Build 38.21.2 before upgrading to Build 42.24.0.
BGW 10.1	42.4.0	Yes	Yes	AA 10.1, CM 10.1 AA 8.1.x, CM 8.1.x AA 8.0.x, CM 8.0.x You can upgrade to Release 10.1 Build 42.4.0 and later from Build 38.20.0 or earlier only after installing Release 7.1.0.5 Build 38.21.3.

Table continues…

Firmware version	Build	v1, v2	v3	Recommended Communication Manager version
BGW 8.1.x	41.38.0	Yes	Yes	AA 8.1.x, CM 8.1.x AA 8.0.x, CM 8.0.x AA 7.1.x, CM 7.1.x AA 7.0.x, CM 7.0.x + You can upgrade to Release 8.1.x Build 41.24.0 and later from Build 38.20.0 or earlier only after installing Release 7.1.0.5 Build 38.21.3.
BGW 8.1	41.9.0	Yes	Yes	AA 8.1, CM 8.1 AA 8.0, CM 8.0 AA 7.1.x, CM 7.1.x AA 7.0.x, CM 7.0.x + You can upgrade to Release 8.1 Build 41.9.0 and later from Build 38.20.0 or earlier only after installing Release 7.1.0.5 Build 38.21.3.
BGW 8.0	40.10.1	Yes	Yes	AA 8.0, CM 8.0 AA 7.1.x, CM 7.1.x AA 7.0.x, CM 7.0.x + AA 6.3.x, CM 6.3.x + You can upgrade to Release 8.0 Build 40.10.1 and later from Build 38.20.0 or earlier only after installing Release 7.1.0.5 Build 38.21.3.
BGW 7.1.3.x	39.x.y	Yes	Yes	AA 7.0 FP 1, CM 7.0.1 AA 7.0, CM 7.0+ AA 6.2 FP 4, CM 6.3.6+ AA 7.1, CM 6.3.x, AA 7.0, CM 7.1.3 You can upgrade to Release 7.1.3 Build 39.16.0 and later 39.x.y from Build 38.20.0 and earlier only after installing Release 7.1.0.5 Build 38.21.3.

Table continues…

Firmware version	Build	v1, v2	v3	Recommended Communication Manager version
BGW 7.1.2	39.x.y	Yes	Yes	AA 7.0 FP 1, CM 7.0.1 AA 7.0, CM 7.0+ AA 6.2 FP 4, CM 6.3.6+ AA 7.1, CM 6.3.x, AA 7.0, CM 7.1.2 You can upgrade to Release 7.1.2 Build 39.12.0 and later 39.x.y from Build 38.20.0 and earlier only after installing Release 7.1.0.5 Build 38.21.3.
BGW 7.1.0+	38.16.0+	Yes	Yes	AA 7.0 FP 1, CM 7.0.1 AA 7.0, CM 7.0+ AA 6.2 FP 4, CM 6.3.6+ AA 7.1, CM 6.3.x, AA 7.0 Branch Gateway requires a 7.x build (37+) to successfully upgrade to Build 38.8.0 or later. Earlier builds will fail with the `Invalid file` error type. If Branch Gateway is running 36.x or earlier build, you must upgrade to 37.x.y before upgrading to 38.x.y.
BGW 7.0.1.2	37.41.0	Yes	Yes	AA 7.0 FP 1
BGW 7.0.1.1	37.39.0	Yes	Yes	AA 7.0, CM 7.0
BGW 7.0.1	37.38.0	Yes	Yes	AA 7.0 FP 1, CM 7.0.1 AA 6.2 FP 4, CM 6.3.6 AA 7.0, CM 7.0
BGW 7.0.0.2	37.21.0	Yes	Yes	AA 7.0, CM 7.0 AA 6.2 FP 4, CM 6.3.6+
BGW 7.0.0.1	37.20.0	Yes	Yes	AA 7.0, CM 7.0 AA 6.2 FP 4, CM 6.3.6+
BGW 7.0	37.20.0	Yes	Yes	AA 7.0, CM 7.0 AA 6.2 FP 4, CM 6.3.6+
BGW 6.3.14	36.18.0	Yes	Yes	CM 6.3.x,AA 7.0
BGW 6.3.7+	36.16.0+	Yes	Yes	AA 6.2 FP 4, CM 6.3.6+
BGW 6.3.6 JITC	36.x.y	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+

Table continues…

Firmware version	Build	v1, v2	v3	Recommended Communication Manager version
BGW 6.3.5	35.x.y	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 6.3.1	34.6.0+	Yes	Yes (min FW build 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	33.13.0	Yes	No (base not supported)	AA 6.2 FP2-CM 6.3 - May 2013
BGW 6.2.1	32.26.0	Yes	No (base not supported)	AA 6.2 FP1-CM 6.2 sp4 - Dec 2012

Branch Gateway features

The following table summarizes G450 Branch Gateway features. Some features are supported only in the IPv4 environment.

Feature type	Supported features
Hardware features	• 9-slot chassis (one slot for main board and eight slots for media modules) • Swappable main board module • Hot-swappable media modules • Support for hot-swappable external compact flash • Support for two load sharing hot-swappable power supply units • Hot-swappable fan tray • VoIP DSPs (up to 320 channels) • Memory SIMMs (G450 v1, v2, v3)
Voice features	• H.248 gateway • Voice line interfaces: - IP phones - Analog phones - Avaya DCP phones - BRI Phones - FXS/Fax - VoIP - Fax and modem over IP • Voice trunk interfaces: - FXO

Table continues…

Feature type	Supported features
	- BRI - T1/E1 • Supported CODECs: G.711A/μLaw, G.729a, G.726, Opus codec • Survivability features for continuous voice services: - Local Survivable Processor (LSP) with S8300 - Standard Local Survivability (SLS) (IPv4 only) - Emergency Transfer Relay (ETR) - Modem Dial Backup - Dynamic Call Admission Control (CAC) for Fast Ethernet, Serial, and GRE tunnel interfaces - Inter-Gateway Alternate Routing (IGAR) • DHCP and TFTP server to support IP phones images and configuration (IPv4 only) • Announcements support • Contact Closure support • International tone detection and generation for DTMF, R1-MF, R2-MFC, call classification support • Custom tone detection and generation support **Note:** IPv6 is not supported on WAN.
Routing and WAN features	• Two WAN 10/100 Ethernet ports with traffic shaping capabilities • T1/E1 and USP interfaces for G450 Branch Gateway v1, v2, v3 • PPPoE (IPv4 only), Frame-relay, and PPP (IPv4 only) • Routing Protocols: Static, OSPF, RIP • VRRP (IPv4 only) • Equal Cost Multi Path routing (ECMP) • IPSec VPN • CRTP • WAN Quality of Service (QoS) • Policy-based routing • DHCP relay • GRE tunneling • Dynamic IP addressing (DHCP client/PPPoE) • Object tracking

Table continues…

Feature type	Supported features
	• Backup Interface
LAN features	• Two LAN 10/100/1000 RJ-45 Ethernet ports (w/o POE) • Auto-negotiation • 4K MAC table with aging • 64 VLANs • Multi-VLAN binding, 802.1Q support • Ingress VLAN Security • Broadcast/Multicast storm control • Automatic MAC address aging • Rapid Spanning Tree • Port mirroring • RMON statistics • Port redundancy • LLDP (IPv4 only)
Security hardened hardware features	• Media and signaling encryption • Secured management • Digitally signed gateway firmware • Managed security service support • Access list support
Management features	• Avaya Device Manager • RADIUS Authentication support (IPv4 only) • SNMPv1 traps and SNMPv3 notifications • Telnet (IPv4 only) and SSHv2 support • SCP, TFTP, FTP, and HTTP/HTTPS clients • Syslog client • Modem access for remote administration • Packet Sniffing • RTP-MIB • Backup and Restore on USB Flash drive

G450 Branch Gateway physical description

G450 Branch Gateway has four hardware versions, G450 1.x, G450 2.x, G450 3.x, and G450 4.x. The G450 Branch Gateway hardware suffix printed on the label on the rear of the chassis (1.x, 2.x, 3.x, or 4.x) corresponds to versions 1, 2, 3, and 4 respectively.

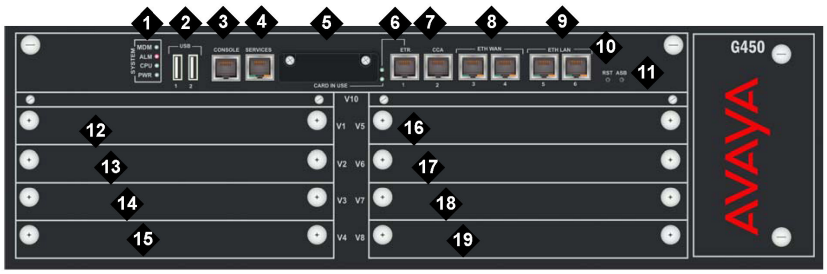


Figure 1: Branch Gateway G450 1.x Chassis

No	Name	Description
1	System (SYSTM) LEDs	LEDs that indicate status of the system.
2	USB	USB ports for the system.
3	CONSOLE (CNSL)	RS-232 port for services and maintenance access. RJ-45 connector.
4	SERVICES (SVCS)	Ethernet 10/100 port for services and maintenance access. RJ-45 connector.
5	CARD IN USE (CF BSY) / COMPACT FLASH (CMPCT FLSH) LED	Compact flash slot.
6	ETR	Emergency Transfer Relay port that controls two external 808A emergency transfer panels. RJ-45 connector.
7	CCA	RJ-45 port for ACS (308) contact closure adjunct box.
8	ETH WAN	Two 10/100 Base TX Ethernet WAN ports. RJ-45 connectors.
9	ETH LAN	Two 10/100/1000 Base TX Ethernet LAN ports. RJ-45 connectors.
10	RST	Reset button. Resets the chassis configuration.
11	ASB	Alternate Software Bank button. Reboots G450 Branch Gateway with the software image in the alternate bank.
12	V1	Slot for standard media module or S8300 Server.
13	V2	Standard media module slot.
14	V3	Standard media module slot.
15	V4	Standard media module slot.
16	V5	Slot for standard media module or S8300 Server.
17	V6	Standard media module slot.

Table continues…

No	Name	Description
18	V7	Standard media module slot.
19	V8	Standard media module slot.

Related links

Supported media modules on page 21

Chapter 3: What's new in Branch Gateway

This chapter provides an overview of the new and enhanced features of Branch Gateway Release 10.2.x.

For more information about these features and administration, see:

- *Administering Avaya G450 Branch Gateway*
- *Avaya G450 Branch Gateway CLI Reference*

New in Branch Gateway Release 10.2

The following section describes new features and enhancements that are available in Branch Gateway 10.2.

TLS 1.3

With Release 10.2, Branch Gateway supports TLS 1.3.

Removed the ip license-server command

From Release 10.2, discontinued support for licensing of Communication Manager Release 5.2.1 and earlier, use Communication Manager Release 10.1.x and later with Branch Gateway Release 10.2.

New commands in G450 Branch Gateway

Release 10.2 adds the following Command-line interface (CLI) commands to configure the Branch Gateway:

- **`snmp-server test trap`**: Command to send a test trap to configured destinations.
- **`set server-blade-monitoring`**: Command to control the heartbeat monitoring of an S8300 server in slot v1 and slot v5.
- **`show server-blade-monitoring`**: Command to display monitoring process of an S8300 server.
- **`server-blade-vlan`** - Command to set the main VLAN for the server in the selected slot.
- **`show server-blade-vlan`**: Command to display the server-blade-vlan.
- **`server-blade-oob-vlan`**: Command to set Out Of Band management VLAN for the server in the selected slot.
- **`no server-blade-oob-vlan`**: Command to clear the Out of Band management VLAN for a server in the selected slot.

- **`show server-blade-oob-vlan`**: Command to display the status of server-blade-vlan configured as the ICC Out of Band management interface.

Branch Gateway feature matrix

The following table lists the feature matrix of Branch Gateway from Release 7.1.x to Release 10.2.x. The features listed in the table covers the key features only.

Feature name	Release 7.1.2 or 7.1.3	Release 8.0	Release 8.1.x	Release 10.1	Release 10.2.x
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y	Y
16-digit dial plan extension	N	Y	Y	Y	Y
Login authentication password complexity	N	Y	Y	Y	Y
Syslog over TLS	N	N	Y	Y	Y
Support of DC power supply forG450 Branch Gateway	N	N	Y	Y	Y
Edge Gateway mode	N	N	N	Y	Y
Support of TLS 1.3	N	N	N	N	Y

Chapter 4: Optional components

Supported media modules

You can install up to eight media modules on a G450 Branch Gateway.

Media module	Description
S8300	Communication Manager server
Telephony media modules	
MM711	8 universal analog ports
MM714	4 analog telephone ports and 4 analog trunk ports
MM714B	4 analog telephone ports, 4 analog trunk ports, and an emergency transfer relay
MM716	24 analog ports
MM712	8 DCP telephone ports
MM717	24 DCP telephone ports
MM710, MM710B	1 T1/E1 ISDN PRI trunk port
MM720	8 ISDN BRI trunk or endpoint (telephone or data) ports
MM721	8 ISDN BRI trunk or endpoint (telephone or data) ports
MM722	2 ISDN BRI trunk ports
WAN media modules (not supported in G450 Branch Gateway v4)	
MM340	1 E1/T1 data WAN port
MM342	1 universal serial data WAN port

Related links

G450 Branch Gateway physical description on page 17

Media module slot configuration

Before installing media modules in Branch Gateway chassis, it is considered that each media module type can be housed in a certain slot.

G450 Branch Gateway chassis has eight media module slots, marked V1, V2, V3, V4, V5, V6, V7, and V8. The following table lists compatible slots for each media module type.

Media module	Permitted slots
MM340	V3, V4, V8
MM342	V3, V4, V8
MM710	Any media module slot, V1-V8
MM711	Any media module slot, V1-V8
MM712	Any media module slot, V1-V8
MM714	Any media module slot, V1-V8
MM714B	Any media module slot, V1-V8
MM716	Any media module slot, V1-V8
MM717	Any media module slot, V1-V8
MM720	Any media module slot, V1-V8
MM721	Any media module slot, V1-V8
MM722	Any media module slot, V1-V8
S8300	V1

G450 Branch Gateway media module capacity

G450 Branch Gateway chassis provides a simultaneous support of the following:

- Up to eight telephony media modules: MM710, MM711, MM712, MM714, MM714B, MM716, MM717, MM720, MM722.
- Up to three WAN media modules: MM340 and MM342.

  G450 Branch Gateway v4 does not support MM340 and MM342.
- One S8300 Server.

S8300E Server hardware specifications

The hardware for S8300E Server as a primary controller is identical to the hardware for S8300E Server as a survivable remote server. The difference between the two configurations is only in the software.

S8300E Server is a dual core Intel Ivy Bridge processor.

S8300E Server resides in Branch Gateway slot V1 and includes the following:

- 320-GB, 500-GB, or 1-TB HDDD
- 500-GB SSD
- 2 8-GB of DDR3 SDRAM
- 512-KB L2 cache and 4-MB L3 cache
- 3 USB 2.0 ports

- External Ethernet LAN port
- USB port for DVD Drive
- Services Ethernet port

Telephony media modules

Branch Gateway supports MM711, MM714, MM714B, and MM716 analog media modules, MM712 and MM717 DCP media modules, the MM710B E1/T1 media module, MM720, MM721 and MM722 BRI media modules.

MM711 media module specifications

The MM711 media module provides analog trunk and phone features and functionality.

The administrator can configure MM711 ports as follows:

- Central office trunk, either loop start or ground start
- Analog Direct Inward Dialing (DID) trunks, either wink-start or immediate-start
- 2-wire analog outgoing CAMA E911 trunks for connectivity to PSTN
- MF signaling for CAMA ports
- Analog, tip/ring devices, such as single-line phones, with or without a LED message waiting indicator

Other MM711 media module hardware features include the following:

- Three ringer loads, which is the Ringer Equivalency Number (REN), for the following loop lengths:
  - 20,000 feet (6096 meters) with a 0.65 mm wire
  - 16,000 feet (4877 meters) with a 0.5 mm wire
  - 10,000 feet (3048 meters) with a 0.4 mm wire

  With ringer load of .1 or less, the supported loop length is 20,000 feet (6096 meters) with a 0.65 mm, 0.5 mm, and 0.4 mm wire.
- Up to eight simultaneously ringing ports

  Branch Gateway supports this number of ports by staggering ringing and pauses between two sets of up to four ports.
- Type 1 Caller ID
- Ring voltage generation for a variety of international frequencies and cadences

MM714 media module specifications

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

Note:

You cannot use four analog trunk ports for analog DID trunks. You must use four analog telephone ports instead.

You can configure MM714 trunk ports as the following:

- A loop start, or a ground start central office trunk with a loop current of 18 to 120 mA
- A two-wire analog outgoing CAMA E911 trunk, for connectivity to PSTN. MF signaling is supported for CAMA ports.

You can configure the 4 MM714 line ports as the following:

- A wink-start or an immediate-start DID trunk
- Analog tip/ring devices, such as single-line phones, with or without a LED message waiting indicator

Other MM714 media module hardware features include the following:

- Three ringer loads, which is the Ringer Equivalency Number (REN), for the following loop lengths:
  - 20,000 feet (6096 meters) with a 0.65 mm wire
  - 16,000 feet (4877 meters) with a 0.5 mm wire
  - 10,000 feet (3048 meters) with a 0.4 mm wire

  With ringer load of .1 or less, the supported loop length is 20,000 feet (6096 meters) with a 0.65 mm, 0.5 mm, and 0.4 mm wire.
- Up to four simultaneously ringing ports
- Type 1 caller ID and Type 2 caller ID
- Ring voltage generation for a variety of international frequencies and cadences

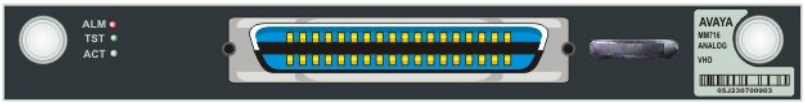
MM714B media module specifications

The MM714B analog media module provides all MM714 features. Additionally, it supports emergency transfer relay (ETR) services by connecting trunk port 5 and line port 4.

MM716 media module specifications

The MM716 media module provides 24 analog ports supporting phones, modem, and fax. You can also configure these ports as DID trunks with either a wink-start or immediate-start signaling. The

24 ports are provided through a 25-pair RJ21X amphenol connector, which you can connect by an amphenol cable to a breakout box or punch-down block.



You can configure MM716 ports as the following:

- Analog tip/ring devices, such as single-line phones, with or without a LED message waiting indicator
- A wink-start or immediate-start DID trunk

Other MM716 media module hardware features include the following:

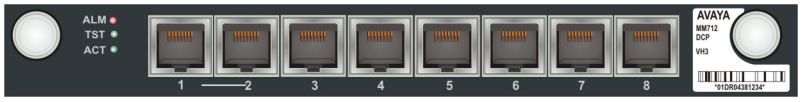
- Three ringer loads, which is the Ringer Equivalency Number (REN), for the following loop lengths:
  - 20,000 feet (6096 meters) with a 0.65 mm wire
  - 16,000 feet (4877 meters) with a 0.5 mm wire
  - 10,000 feet (3048 meters) with a 0.4 mm wire

  With ringer load of .1 or less, the supported loop length is 20,000 feet (6096 meters) with a 0.65 mm, 0.5 mm, and 0.4 mm wire.
- Up to 24 simultaneously ringing ports
- Type 1 caller ID
- Ring voltage generation for a variety of international frequencies and cadences

The MM716 media module is compatible with Avaya Aura® Communication Manager Release 3.1 and later, and Branch Gateway firmware version 29.x.x and later.

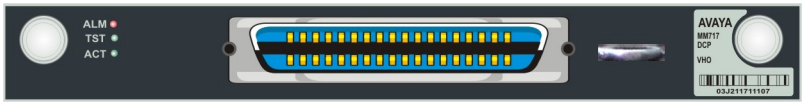
MM712 media module specifications

The MM712 DCP media module provides eight DCP telephone ports. The ports support two-wire Digital Communications Protocol (DCP) phones. For a list of compatible DCP phones, see Supported Avaya phones on page 52.



MM717 media module specifications

The MM717 DCP media module provides 24 DCP ports of two-wire DCP functionality exposed as a single 25-pair amphenol connector. The DCP ports are exposed by connecting the module through a standard amphenol cable to a punch-down block with RJ-11 jacks. The MM717 media module allows you to use one of the smaller media module slots for a large number of DCP phones.



MM710B media module specifications

The MM710B E1/T1 media module terminates an E1 or T1 trunk. The MM710 media module has a built-in Channel Service Unit (CSU), therefore, an external CSU is not necessary. The CSU is only used for the T1 circuit.

Note:

The information in this section applies to the MM710 media module as well.

The MM710B media module provides the following features:

- ISDN PRI capability (23B+D or 30B+D)
- Trunk signaling to support US and International CO, or tie trunks
- Echo cancellation in either direction

MM720 media module specifications

The MM720 BRI media module provides eight ports with RJ-45 jacks that you can administer either as BRI trunk connections or BRI endpoint (phone and data module) connections.

You cannot administer the MM720 BRI media module to support both BRI trunks and BRI endpoints at the same time. However, the MM720 BRI media module supports combining both B-channels together to form a 128-kbps channel. Avaya Aura® Communication Manager 3.1 enables combining B-channels using BONDing to form a higher bandwidth connection. If you administer the MM720 BRI media module to support BRI endpoints, it will not function as a clock synchronization source.

For BRI trunking, the MM720 BRI media module supports up to eight BRI interfaces to the central office at the ISDN TE reference point. The data is transmitted in the following ways:

- Over two 64-kbps channels, called B1 and B2, which can be circuit-switched simultaneously.
- Over a 16-kbps channel, called the D-channel, which is used for signaling. The MM720 media module occupies one time slot for all eight D channels.

The circuit-switched connections have an A- or Mu-law option for voice operation. The circuit-switched connections operate as 64-kbps clear channels in Data mode.

For BRI endpoints, the MM720 BRI media module supports up to 16 BRI stations and data modules that conform to AT&T BRI, World Class BRI, and National ISDN NI1/NI2 BRI standards. The MM720 BRI media module provides 40-volt phantom power to BRI endpoints.

MM721 media module specifications

The MM721 Basic Rate Interface (BRI) media module has eight ports. You can administer these ports either as BRI trunk or BRI endpoint connections, such as a phone and data module.

You cannot administer the MM721 BRI media module to support both BRI trunks and BRI endpoints at the same time. You can use all eight ports on the MM721 media module only for stations or trunks. You cannot use a mixture of ports for both applications.

For BRI trunking, the MM721 BRI media module supports up to eight BRI interfaces to the central office at the ISDN S/T reference point.

For BRI endpoints, each of the eight ports on the MM721 BRI media module supports integrated voice and data endpoints for up to 2 BRI stations or data modules or both. The MM721 BRI media module provides 48-volt phantom power to BRI endpoints.

The MM721 BRI media module supports 4-wire S/T ISDN BRI on each interface.

The MM721 BRI media module transmits data in the following ways:

- Over two 64-kbps channels called B1 and B2. You can circuit-switch these channels simultaneously.
- Over a 16-kbps channel called the D-channel, which is used for signaling.

The circuit-switched connections have an A-law or Mu-law option for voice operation. In Data mode, circuit-switched connections operate as 64-kbps clear channels.

The MM721 BRI media module is compatible with Avaya Aura® Communication Manager Release 6.0.1 and later and Branch Gateway firmware version 31.18.1 and later.

MM722 media module specifications

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. Data is transmitted in the same way as for the MM720 media module.

Note:

The MM722 media module does not support BRI stations or combining both B channels together to form a 128-kbps channel.

WAN media modules

G450 Branch Gateway v1, v2, v3 supports the MM340 E1/T1 WAN and MM342 Universal Serial Port WAN media modules.

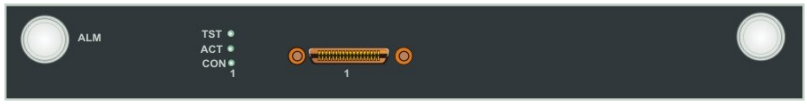
G450 Branch Gateway v4 does not support MM340 and MM342 modules.

MM340 E1/T1 WAN media module

The MM340 E1/T1 WAN media module provides a data WAN access port for the connection of an E1 or T1 WAN.

MM342 universal serial data WAN media module

The MM342 media module provides a universal serial data WAN access port.



The MM342 media module supports the following WAN protocols:

- V.35/ RS449
- X.21

For these connections, the MM342 media module requires one of the following cables:

- Avaya Serial Cable DTE V.35 (Universal Serial Port to V.35)
- Avaya Serial Cable DTE X.21 (Universal Serial Port to X.21)

VoIP modules in G450 Branch Gateway

A media processor or VoIP module provides channels to support voice calls.

G450 Branch Gateway has four VoIP slots. The following table describes supported VoIP modules:

VoIP modules	Description
MP20	Supports a maximum of 20 channels. • Provides 25 VoIP channels for G.711 and G.726. • Provides 20 VoIP channels for G.729.
MP80	Supports a maximum of 80 channels.
MP160	Supports new media services, such as V.150.1, Opus codec, and T.38 fax over SRTP. An MP160 module supports a maximum of 160 channels and 80 channels with the Opus codec.

Configuration matrix

G450 Branch Gateway supports the MP20 and MP80 modules in any configuration for 4 slots and a maximum of 320 channels.

Note:

G450 Branch Gateway v4 does not support the MP20 and MP80 DSP modules. G450 Branch Gateway v4 supports only the MP160 DSP module.

The following table shows allowed combinations of optional VoIP modules for G450 Branch Gateway.

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

G450 Branch Gateway v4 supports only Combination # 1.

Once the installation for MP160 is completed, you can install the MP80/20s module in any of the remaining slots.

Chapter 5: Branch Gateway services

Branch Gateway provides various services, including the following:

- IPv6 support
- Telephony services
- Physical media services
- Media Gateway Controller (MGC) support
- Audio and video features
- LAN and WAN services

IPv6 support

Internet Protocol version 6 (IPv6) is a successor to IPv4. IPv6 supports 128-bit addressing, allowing a larger number of IP addresses. IPv6 also enhances security, simplicity of configuration, and routing performance. IPv6 can coexist with IPv4 networks, facilitating the transition process.

The Internet Engineering Task Force (IETF) published RFC 2460 defines IPv6.

Note:

Some Branch Gateway features are not supported in IPv6.

Addressing

IPv6 provides about $3.4x10^{38}$ unique IP addresses. This eliminates the IPv4 mechanisms, such as Network Address Transitions (NAT), that are used to relieve IP address exhaustion. IPv6 addresses are normally written as hexadecimal digits with colon separators. For example: 2005:af0c:168d::752e:375:4020. The double colon "::" represents a string of zeroes, according to RFC4291.

Routing

IPv6 simplifies the routing process in the following ways:

- Simplified packet header, despite enhanced functionality.
- IPv6 routers do not perform fragmentation. This is carried out by IPv6 hosts.
- IPv6 routers do not need to recompute a checksum when header fields change.
- Routers do not need to calculate the time a packet spent in the queue.

- IPv6 supports stateless address configuration. IPv6 hosts can be configured automatically when connected to a routed IPv6 network through ICMPv6. Stateful configuration using DHCPv6 and static configuration are also available.

Deployment and transition

There are several mechanisms that simplify the deployment of IPv6 running alongside IPv4. The key to the IPv6 transition is dual-stack hosts. Dual-stack hosts refer to the presence of two IP software implementations in one operating system, one for IPv4 and one for IPv6. These dual-stack hosts can run the protocols independently or as hybrids. Hybrid dual-stack hosts are common on recent server operating systems and computers.

Tunelling allows to use IPv4 infrastructure to carry IPv6 packets when an IPv6 host or network must use the existing IPv4 infrastructure. Tunneling can be either automatic or configured. Configured tunneling is more suitable for large, well-administered networks.

Key differences between IPv4 and IPv6

Features	IPv4	IPv6
Address space	32-bit, about $4.3x10^9$	128-bit, about $3.4x10^{38}$
Configuration	Requires DHCP or manual configuration.	Stateless auto-configuration. Does not require DHCP or manual configuration.
Address format	Decimal digits with colon separators, for example: 192.168.1.1	Hexadecimal digits with colon separators. For example: 2005:af0c:168d::752e:375:4020. The double colon “::” represents four zeros “0000”.
Broadcast and Multicast support	Yes	Broadcast is not supported. Various forms of Multicast are supported for a higher network bandwidth efficiency.
QoS support	ToS using DIFFServ	Flow labels and classes

Branch Gateway telephony services

Branch Gateway provides a telephone exchange service, supporting the connection of various phone types and outside telephone lines. Phones and lines are connected to Branch Gateway through media modules on the chassis. Different media modules provide access ports for different phone types and lines.

Telephony services are controlled by a Media Gateway Controller (MGC) running Communication Manager call processing software. You can use Communication Manager to configure advanced telephone exchange features. For more information about Branch Gateway telephony services, see *Administering Avaya Aura® Communication Manager*.

VoIP services

Branch Gateway provides the following VoIP services:

- Up to four VoIP DSPs that provide voice services over IP data networks.
- Use various types of phones and trunks that do not directly support VoIP.
- Translates voice and signaling data between VoIP and the system used by phones and trunks. Avaya media modules convert the voice path of traditional circuits, such as analog trunk, T1/E1, and DCP, to a TDM bus inside Branch Gateway. The VoIP engine then converts the voice path from the TDM bus to a compressed or uncompressed and packetized VoIP over an Ethernet connection.

Branch Gateway provides VoIP services over LAN and WAN. G450 Branch Gateway supports up to four VoIP DSP child boards. The maximum number of supported active channels is 320.

Physical media services

Branch Gateway supports various types of phones, lines, and access ports provided for their connection.

Supported phone types and ports

Branch Gateway supports IP, Avaya DCP, analog, and BRI phones.

You must connect phones to ports supported for the phone type. Different types of phone ports are provided by different media modules. The following table lists which ports you can use to connect each type of phone.

Phone type	Ports
IP phones and softphones	You must connect an external LAN switch to one of the front panel ETH LAN ports. Avaya Aura® Communication Manager processes the phone registration and signaling control information.
Avaya DCP digital phones	DCP ports on the MM712 and MM717 media modules.
Analog phones	Analog line ports on MM711, MM714, MM714B, and MM716 analog media modules.

Related links

Supported media modules on page 21
Supported Avaya phones on page 52

Ports for outside telephone lines

The following table lists which modules you can use to connect each type of outside line.

Line type	Ports
ISDN line	ISDN ports on the MM720, MM721, and MM722 BRI media modules.
Analog trunks	Analog trunk ports on the MM714 or MM714B media module. Universal analog ports on the MM711 media module. DID wink-start and immediate-start trunk ports on the MM716 media module and the four MM714 line ports.
T1/E1 voice lines	The T1/E1 port on the MM710 T1/E1 media module.

Related links

Supported media modules on page 21

Media Gateway Controller

A Media Gateway Controller (MGC) controls Branch Gateway telephony services. MGC can be internal or external to Branch Gateway. An Internal Call Controller (ICC) is an internal MGC. An External Call Controller (ECC) is an external MGC communicating with Branch Gateway over the network.

An Avaya server managed with Avaya Aura® Communication Manager is an MGC for Branch Gateway.

Supported Avaya servers

MGCs supported by Branch Gateway include ECC and ICC.

Avaya Aura® Release 10.1 and later does not support Avaya S8300D Server, Avaya S8800 Server, Dell™ PowerEdge™ R610/ 620/ 630, and HP ProLiant DL360 G7/ G8/ G9.

The following table lists the MGCs that Branch Gateway supports.

MGC	Type	Usage
Avaya S8300E Server	Media module	ICC, ECC, or LSP
Avaya Converged Platform 130 Appliance: Dell PowerEdge R640	External	ECC

Branch Gateway survivability

Branch Gateway provides the following configuration options for continuous phone services:

- You can configure Branch Gateway to use up to four MGCs. Each controller can be configured with an IPv4 and IPv6 address. Each configured address is either an IPv4 address of a TN799 (C-LAN) board connected to the server or an IPv4/IPv6 address of the Communication Manager Processor Ethernet interface. The four addresses are grouped into primary and secondary controllers, using a transition point to separate the two groups.

- Using connection-preserving migration, you can configure Branch Gateway to preserve the bearer paths of stable calls if Branch Gateway migrates to another MGC, including a Local Survivable processor (LSP) also known as Survivable Remote Server (SRS). This also applies to migration back from an LSP to the primary MGC. A call with an established audio path between all parties is considered stable. A call with a one-way audio path is not considered stable and therefore is not preserved. Any change of state leads to ending the call. For example, putting a call on hold during the MGC migration ends the call. Special features, such as conference and transfer, are not available on preserved calls. Connection-preserving migration preserves all types of bearer connections except BRI. PRI trunk connections are preserved.
- You can configure Standard Local Survivability (SLS) to enable a local Branch Gateway to provide a limited MGC functionality when there is not connection to an external MGC. You can also configure SLS from Branch Gateway using a Command Line Interface (CLI). SLS is supported for all analog interfaces, ISDN BRI/PRI trunk interfaces, non-ISDN digital DS1 trunk interfaces (T1 Robbed Bit and E1-CAS), IP phones, IP softphones, and DCP phones. SLS is available only in IPv4.
- You can configure Enhanced Local Survivability (ELS) by installing S8300 in Branch Gateway as a Local Survivable processor (LSP) also known as Survivable Remote Server (SRS). In this configuration, S8300 Server is not a primary MGC but takes over to provide continuous phone services if all external MGCs become unavailable. Active calls continue without interruption when S8300 Server takes over.
- You can configure the dialer interface to connect to Branch Gateway primary MGC by a serial modem if the connection between Branch Gateway and the MGC is lost.
- You can configure Avaya Aura® Communication Manager to support the Auto Fallback feature. A LSP enables Branch Gateway to return to the primary MGC automatically when the connection is restored between Branch Gateway and the MGC. When a LSP services Branch Gateway, it automatically attempts to register with the MGC at periodic intervals. The MGC can deny registration if it is overloaded with call processing or in other configured conditions. By migrating Branch Gateway to the MGC automatically, a fragmented network can be unified more quickly, without manual configuration.

  Auto Fallback does not include survivability. Therefore, there is a short period during the registration with MGC, during which calls are dropped and the service is not available. This problem can be minimized using connection-preserving migration.
- With a dynamic trap manager you can ensure that Branch Gateway sends traps directly to a currently active MGC. If the MGC fails, the dynamic trap manager ensures that traps are sent to a backup MGC.

Communication Manager features

Avaya Aura® Communication Manager provides user and system management functionality, intelligent call routing, application integration, and enterprise communication networking. Communication Manager offers over 700 features.

Communication Manager software applications perform the following functions:

- Determine where to connect your phone call based on the number you dial.
- Assign numbers to local phones.
- Play dial tones, busy signals, and prerecorded voice announcements.
- Enable or prohibit access to outside lines for specific phones.
- Assign phone numbers and buttons to special features.
- Exchange call switching information with older telephone switches that do not support VoIP.

For more information about Avaya Aura® Communication Manager features, see *Administering Avaya Aura® Communication Manager*.

G450 Branch Gateway features

Emergency Transfer Relay

The Emergency Transfer Relay (ETR) feature provides basic telephony services in case of a power outage or failed connection to Communication Manager. ETR services are provided on the MM714B media module by connecting the module trunk port 5 to line port 4. You can also connect two external 808A ETR panels to the Branch Gateway front panel port. Each 808A Emergency Transfer Panel provides emergency trunk bypass or power-fail transfer for up to five incoming trunk loops to five analog phones. It also maintains connections when switching from Emergency Transfer mode to normal operation.

Contact Closure

The Contact Closure feature is a controllable relay providing dry contacts for various applications. To implement Contact Closure, you must connect an Avaya Partner Contact Closure adjunct box to the CCA port on the Branch Gateway chassis. The adjunct box provides two contact closures that can be operated in either a “normally closed” or “normally open” state. Contact closures can control peripheral devices, for example, devices that automatically lock or unlock doors, or voice recording units. You can configure the CCA port so that the connected devices are controlled by an endpoint device, such as a phone. For example, a user can unlock a door by entering a sequence of digits on a phone keypad.

Fax, modem, and TTY over IP

Branch Gateway supports fax, modem, and TTY over IP.

T.38 Fax Fallback to G.711

The T.38 Fax Fallback to G.711 feature provides the functionality for enterprise networks managed by Communication Manager to interoperate with older Verizon networks that do not support T.38

Fax for fax transport. A new codec type, T.38 Fax with Fallback to G.711 Pass-Through, is added to the IP codec set for Fax mode.

T.38 Fax Fallback to G.711 operates in the following way:

- The call connection is signaled for a standard T.38 fax relay.
- If T.38 fax relay is successfully negotiated, Communication Manager issues a re-INVITE to G.711 mode.
- The fax call is in G.711 mode until the user disconnects. This feature works only over SIP trunks.

For more information about the T.38 Fax Fallback to G.711 feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

T.38 with Error Correction mode

T.38 with Error Correction mode (ECM) corrects errors without retransmitting multiple pages.

Communication Manager instructs Branch Gateway to use ECM as a part of T.38 Fax exchange in the following cases:

- The local media gateway indicates support for this feature through exchange capability.
- The IP codec set is set to **T.38-standard**.
- ECM is enabled.

Fax machines with the memory capacity to store page data can use ECM for error-free page transmission. When ECM is enabled, a fax page is transmitted in a series of blocks that contain frames with data packets. After receiving data for a complete page, a receiving fax machine notifies the transmitting fax machine of any frames with errors. The transmitting fax machine then retransmits the specified frames. This process is repeated until all frames are received without errors.

If the receiving fax machine is unable to receive an error-free page, the fax transmission fails and one of fax machines is disconnected.

For more information about the T.38 with ECM feature, see *Administering Network Connectivity on Avaya Aura® Communication Manager*.

T.38 fax Transport over RTP/SRTP

The default T.38 Fax relay feature employs the use of UDPTL transport which does not provide any encryption support. From Release 10.1, page 2 of the IP Codec-Set screen on the Communication Manager SAT interface allows you to administer SRTP transport for T-38 fax. This feature will provide the same encryption technique and strength as Avaya supports for voice and video transport.

Note:

This feature is not supported in G450 gateways that include MP80 and MP20 modules. Only MP160 DSPs are supported.

V.150.1 Modem over IP

The V.150.1 Modem over IP (MoIP) feature is an industry-standard compliant V-series MoIP transport for carrying modem traffic over an IP network and supporting interoperability with secure third-party terminal devices.

The V.150.1 MoIP feature supports the following modem modulation modes:

- V.32 and V.34 up to 33.6 Kbps
- V.90 and V.92 up to 56 Kbps

V.150.1 MoIP performs the following functions:

- Transforms analog-tone events into digital-control messages, so that the protocol can pass over hops.
- Recovers from failover and operates at a higher speed up to V.92 as the protocol is sent in sequenced packets.
- Interoperates with various vendors.
- Eliminates extra trunking because of data, voice, and fax convergence.

The MP160 DSP card is required to support V.150.1 Modem over IP feature.

G450 Branch Gateway supports mixed DSP boards of different DSP channel capacities. The number of DSP channels on G450 Branch Gateway must not exceed 320.

For more information about V.150.1 MoIP and the MP160 DSP daughter board, see *Configuring V.150.1 on Avaya G450 and G430 Branch Gateway*.

Service Level Agreement Monitor

Service Level Agreement (SLA) Monitor is an integrated set of tools designed to obtain high audio and video performance in a converged network. SLA Monitor communicates with IP telephony components and other sources through a web-based server application. With the data gathered by SLA Monitor, you can check the network contribution to the performance of audio and video applications.

SLA Monitor performs the following functions:

- Corrects Differentiated Services issues.
- Handles rogue applications.
- Provides real-time visibility to live sessions.

The SLA Monitor agent is a component of SLA Monitor. The agent participates in enterprise end-to-end monitoring and troubleshooting of various types of network issues that affect IP telephony. The SLA Monitor agent can trace packets from source to destination. The SLA Monitor agent can also monitor Differentiated Services markings at each hop as the packets travel through the network.

G450 Branch Gateway acts as a SLA Monitor agent.

The SLA Monitor server collects router-flow data, as well as data from SLA Monitor agents, to provide a clear picture of how the network and media elements contribute to end-to-end quality.

List Trace and List Measurement

The List Trace and List Measurement commands provide additional performance and diagnostic information for V.150 / Modem-over-IP calls.

The standard List Trace command provides logging information for the V.150.1 call state, reducing dependency on Wireshark captures and other logging tools.

The List Measurement command aggregates the usage of V.150.1 calls and provides a summary of G.711 equivalent call statistics.

For more information about the List Trace and List Measurement commands, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Edge Gateway mode

H.248 Proxy server

Avaya Aura® solution allows its components (Communication Manager, Session Manager, Session Border Controller, Media Gateways, and IP Phones) to be deployed in a distributed architecture. With the Edge Gateway feature, endpoints and gateways can operate in local NAT address domains at the branch office sites, while the Avaya server products remain in the data centers. The data centers operate in a private address space as well. The Avaya Session Border Controller (ASBCE) is the conversion element that supports end-to-end communication from the data centers to public service provider networks and the branch office sites.

The G4xx gateways operating as an *Edge Gateway* is on the public network side of the firewall from the ASBCE. Avaya products within the data center can communicate with *IP Addresses* whereas, the Edge gateway communicates within a NAT address space. The Edge gateway tunnels H.248 signaling into a TCP/TLS connection towards port 2944 on the ASBCE. The ASBCE acts as an H.248 Proxy server to modify the address fields and forward these messages to TCP port 2944 on Communication Manager.

Edge Gateway to SBC management link

Edge Gateway supports a new management link (MGSBC) with the Session Border Controller. The link is required to support the following:

- SNMP TRAP messages that are sent up a link to UDP port 162 on the host Communication Manager.
- The transport of SSH maintenance messages between a Communication Manager and an Edge gateway.

The Edge gateway establishes a TLS/TCP connection with the TCP port 2946 on the ASBCE when the gateway finishes booting up. This connection occurs before the establishment of the H.248 registration to expand the window of diagnostic capability for the service personnel.

Enabling Edge Gateway mode

To enable Edge mode, use the ‘SBC@ip’ address in the **`set mgc list`** gateway CLI command. For more details on enabling the Edge mode, see the *Avaya Branch Gateway G450 CLI Reference* guide.

Important:

- Before enabling Edge mode, ensure that the gateway is connected with an Avaya Session Border Controller Release 10.1 or later and a Communication Manager Release 10.1 or later.
- From Release 10.1 the S8300 server applications do not support deployment behind a NAT. Only the G450 Branch Gateway with the supported analog / digital sets, trunks, and SIP endpoints can be used. Remove the S8300 server if you convert an existing branch to an edge friendly configuration.
- This feature is not supported in G450 gateways that include MP80 and MP20 modules. Only MP160 DSPs are supported.

Additional features

H.248 registration source port

You can define the source port range that Branch Gateway uses when registering with Communication Manager using the following CLI commands:

- **`set registration source-port-range`**
- **`show registration source-port-range`**
- **`set registration default source-port-range`**

If you do not specify the source port range, Branch Gateway selects a port within the default range of 1024 through 65535.

For more information about these commands, see *Avaya Branch Gateway G450 CLI Reference*.

Accessing diagnostic logs

You can access diagnostic logs using the following CLI commands:

- **`show all logs`**
- **`show event-log`**
- **`system show reset-log`**
- **`show dev log file`**

For troubleshooting, you must send the diagnostic logs to Avaya technical support team.

For more information about accessing diagnostic logs and the related CLI commands, see *Administering Avaya G450 Branch Gateway* and *Avaya Branch Gateway G450 CLI Reference*.

LAN services

You can use Branch Gateway as a LAN switch. You can also integrate Branch Gateway into an existing LAN.

LAN physical media

Branch Gateway provides LAN services through the fixed LAN ports on the chassis front panel for the connection of external LAN switches or local data devices. LAN ports are connected to an internal LAN switch and support HP auto-MDIX, which automatically detects and corrects the polarity of crossed cables. This simplifies LAN installation and maintenance.

VLAN configuration

In Branch Gateway, you can configure VLANs on fixed LAN ports.

G450 Branch Gateway supports up to 24 VLANs.

The following VLAN features are supported:

- VLAN port grouping. You can use port VLANs to group LAN ports into logical groups.
- Ingress VLAN Security. You can configure a list of ingress VLANs on each port. Any received packets tagged with an unlisted VLAN are dropped.
- Class of Service (CoS) tagging. Packets are tagged with VLANs with respect to CoS.
- Inter-VLAN routing. You can configure specific VLANs to enable access to WAN and others to deny access to WAN.

Rapid Spanning Tree Protocol

The IEEE 802.1D (STP) and IEEE 802.1w Spanning Tree Protocols (RSTP) are supported on ETH LAN ports.

Port mirroring

Branch Gateway support network traffic monitoring by port mirroring. You can configure port mirroring on any LAN port. You can implement port mirroring by connecting an external traffic probe device to one of the LAN ports. The probe device monitors traffic that is sent and received through other ports by copying the packets and sending them to the monitoring port.

Port redundancy

You can configure port redundancy on Branch Gateway. Port redundancy enables you to provide both a primary link and a backup link to a resource.

Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) simplifies network troubleshooting and enhances the ability of network management tools to discover and maintain network topologies in multi-vendor

environments. LLDP defines a set of advertisement messages (TLVs), a protocol for transmitting TLVs, and a method for storing the information in received TLVs.

As a result, stations attached to a LAN can advertise information about the system and station point of attachment to other stations in the same LAN. This information can be reported to the management station through SNMP MIBs.

The front panel ETH LAN ports support LLDP.

WAN services

Branch Gateway has an internal router and provides direct access to outside WAN lines. You can use Branch Gateway as an endpoint device for a WAN line. You can also use Branch Gateway as a router for the WAN line with an external endpoint device.

Certain WAN services are supported only in IPv4.

WAN physical media

To use Branch Gateway as an endpoint device for WAN, you must install a WAN media module and connect the WAN line to a port on the media module. When you connect a WAN line to the media module, Branch Gateway serves as an router for the WAN line.

You can also use the fixed ETH WAN Fast Ethernet port as a WAN endpoint by configuring the port interface for PPPoE encapsulation (ADSL modem) or Ethernet-DHCP/static IP (cable modem).

To use Branch Gateway as a router, you must connect the external endpoint device to the ETH WAN port on the Branch Gateway front panel using a standard network cable.

WAN line support

Branch Gateway supports the following types of data WAN lines:

- E1/T1
- Universal Serial Port
- PPPoE (ADSL modem)
- Ethernet-DHCP/static IP (cable modem)

G450 Branch Gateway v4 does not support E1/T1 and Universal Serial Port.

Required media modules for WAN lines

The table below lists which media modules you must install to connect each type of outside WAN line.

WAN line	Media modules
Universal Serial Port	MM342
E1/T1 data lines	MM340
PPPoE (ADSL modem)	Chassis
Ethernet (DHCP/static IP) (cable modem)	Chassis

Related links

Supported media modules on page 21

WAN features

The following table describes Branch Gateway WAN features supported in IPv4.

Feature	Description
Traffic shaping	The traffic shaping function estimates the parameters of the incoming traffic. If the incoming traffic exceeds the defined parameters, Branch Gateway can drop the packets or mark them as low-priority.
PPP over channeled and fractional E1/T1	Branch Gateway can map several PPP sessions to a single E1/T1 interface.
PPP over Universal Serial Port	–
PPPoE	–
Unframed E1	Enables full 2.048 Mbps bandwidth usage.
Point-to-Point Frame Relay encapsulation	Supported over channelized, fractional, or unframed E1/T1 ports or over a Universal Serial Port interface.
Frame Relay LMI	The following Frame Relay LMI types are supported: • ANSI (Annex D) • ITU-T:Q-933 (Annex A0) • LMI-Rev1 • No LMI
Backup functionality	Supported between any type of Serial Layer 2 interface.
Dynamic Call Admission Control (CAC) for Fast Ethernet, Serial, and GRE tunnel interfaces	Dynamic CAC provides enhanced control over the WAN bandwidth. When Dynamic CAC is enabled on an interface, Branch Gateway tells the MGC to block calls when the interface bandwidth is exhausted.

Table continues…

Feature	Description
Quality of Service (QoS)	Branch Gateway uses Weighted Fair VoIP Queuing (WFVQ) as the default queuing mode for WAN interfaces. WFVQ combines weighted fair queuing (WFQ) for data streams and priority VoIP queuing to provide real-time responses required for VoIP. Branch Gateway also supports the VoIP Queue and Priority Queue legacy queuing methods.
Weighted Random Early Detection (WRED)	Branch Gateway uses WRED on its ingress and egress queues to improve the network performance. WRED reduces host transmission speed when the ingress Branch Gateway queues are congested.
Policy	Each interface on Branch Gateway can have four active policy lists: • Ingress Access Control List • Ingress QoS List • Egress Access Control List • Egress QoS List Access control lists defines which packets to forward or block. QoS lists change the DSCP and 802.1p priority of routed packets according to packet characteristics.
Policy-based routing	Branch Gateway features policy-based routing, which uses a policy-list structure to implement a routing scheme based on traffic source, destination, type, and other characteristics. You can use policy-based routing lists (PBR lists) to determine routing of packets that match the rules defined in the list. Common applications include separate routing for voice and data traffic, routing traffic originating from different sets of users through different Internet connections, and defining backup routes for classes of traffic.
RTP Header Compression	Branch Gateway saves the bandwidth using RTP compression. It also enhances the efficiency of voice transmission over the network by compressing the headers of RTP packets, minimizing overhead and delays involved in the RTP implementation.

Table continues…

Feature	Description
TCP Header Compression	Branch Gateway uses TCP header compression to reduce the amount of bandwidth needed for non-voice data. TCP header compression can be applied either as a part of RTP Header Compression through IPCH, or using the Van Jacobson method defined in RFC 1144.
Inter-Gateway Alternate Routing (IGAR)	Branch Gateway uses PSTN as an alternative to the WAN interface under certain definable conditions. In providing an alternate routing mechanism, IGAR preserves the call internal makeup so that it can be successfully terminated to its original internal destination.

Data and routing features

Branch Gateway has an internal router. You can configure the following features on the router:

Note:

Features labeled '*' are available only in IPv4.

- Interfaces*
- Routing table
- VPN
- GRE tunneling*
- DHCP and BOOTP relay*
- DHCP server is available in IPv4.
- DHCP client*
- Broadcast relay
- ARP table
- ICMP errors
- RIP*
- OSPF*
- Route redistribution
- VRRP*
- Fragmentation
- Static routes
- Policy-based routing*
- Distribution lists
- Dynamic IP addresses

- DNS resolver
- Unnumbered IP interfaces
- SYN cookies
- Keepalive packets
- Object tracking
- Backup interfaces

Chapter 6: Management, security, alarms and troubleshooting

Branch Gateway Command Line Interface

You can use CLI to configure Branch Gateway and its media modules. CLI is a textual command-prompt interface. It is similar to the command-line interface of other network devices.

You can access CLI using one of the following methods:

- A console device connected to the Console (CNSL) or Services (SVCS) port on the Branch Gateway front panel.
- SSH, which you can use to establish a secure remote session over the network, Services (SVCS) port, or dial-in modem (PPP).

  SSH is enabled by default.
- Telnet through the network.
- Telnet through dialup, using a dialup PPP network connection.

  Telnet is disabled by default on Branch Gateway.

Telnet and the Services port are supported in IPv4.

For information about CLI commands, see *Avaya Branch Gateway G450 CLI Reference*.

For information about how to perform specific configuration tasks using CLI, see *Administering Avaya G450 Branch Gateway*.

Management security features

Branch Gateway supports the following management security mechanisms:

- A basic authentication mechanism, in which users have passwords and privilege levels.
- Support for user authentication provided by an external RADIUS server.
- SNMPv3 user authentication.
- Secure data transfer through SSH and SCP with user authentication.

- EASG authentication for remote service access. EASG is a challenge-response authentication method, which is more secure than password authentication and does not require a static password.
- Management access restriction to an out-of-band interface, LAN or WAN.

Network security features

Branch Gateway provides the following network security features:

- Private secure connections can be configured between Branch Gateway and a remote peer using Virtual Private Network (VPN). VPN at the IP level is deployed using IPSec.
- Protection against DoS (Denial of Service) attacks is provided through:
  - MSS notifications (IPv4 only). Branch Gateway identifies predefined or customer-defined traffic patterns as suspected DoS attacks and generates SNMP notifications, or Managed Security Services (MSS) notifications. Branch Gateway intercepts MSS notifications and under certain conditions forwards them to the Avaya Security Operations Center (SOC) as INADS alarms. The SOC is an Avaya service group that handles DoS alerts, responding to any DoS attack or related security issues.
  - SYN cookies, which protect against a TCP/IP attack.
- From Release 7.0, Branch Gateway supports TLS 1.2. TLS 1.2 provides a higher level of security than earlier versions to protect users from known attacks.

  The TLS protocol provides the following services to all TLS applications:

  - Encryption
  - Authentication
  - Data integrity

  TLS certificate validation is time-zone specific based on the values administered in Avaya Aura® Communication Manager.

Alarms and troubleshooting

Branch Gateway provides various features for error detection, alarms, and troubleshooting. Detailed diagnostic information and troubleshooting are provided by software-based solutions accessible to laptops in the field or remotely from an administrator’s computer. For more information about configuring and using these solutions, see *Administering Avaya G450 Branch Gateway*.

Front panel LEDs

LEDs on the Branch Gateway front panel and their media modules indicate the system and subsystem state. When an issue occurs, LEDs indicate that a technician’s assistance is needed.

Automatic error detection

In normal operation, the Branch Gateway firmware and software automatically detects and attempts to resolve error conditions. Branch Gateway detects errors in the following ways:

- By a firmware test of system components during ongoing operations.
- By a periodic or scheduled software test.

A technician can run more comprehensive tests on demand.

SNMP

Branch Gateway reports alarms using SNMP traps. Branch Gateway fully supports SNMPv1 and SNMPv3.

Note:

SNMP is supported only in IPv4.

Packet sniffing

Branch Gateway features packet sniffing in IPv4 and IPv6. All IP and ARP packets that pass through Branch Gateway are recorded. The recorded packets are stored in a file that you can upload to an Avaya server or computer. Ethereal or Wireshark analyzes recorded packets for troubleshooting purposes.

VoIP debugging using RTP-MIB

Branch Gateway supports the RTP-MIB feature for debugging QoS-related problems across the VoIP network without any specific hardware. In each RTP stream, counters representing various QoS metrics increase when the configured metrics thresholds are exceeded. Branch Gateway stores a limited history of the QoS metric statistics for active and terminated RTP streams. You can use the Branch Gateway CLI to view the statistics.

You can also configure Branch Gateway to send SNMP traps to the SNMP trap manager on an Avaya server at the session termination of each RTP stream that has QoS problems. The Communication Manager SNMP trap manager converts traps to syslog messages and stores them on the Avaya server hard disk.

System logging

System logging is a method of collecting system messages from system events. The Branch Gateway includes a logging package that collects system messages in several output types. Each of these types is called a sink. When the system generates a logging message, the message can be sent to each sink you enable.

System messages do not always indicate errors. Some messages are informational, while others may help to diagnose problems with communications lines, internal hardware, and system software. The logging facility logs configuration commands entered through the CLI or SNMP, system traps, and informative messages concerning the functioning of various processes.

Chapter 7: Branch Gateway capacities

G450 Branch Gateway maximum capacities

Item	Capacity	Description
Maximum number of G450 Branch Gateways controlled by Avaya Aura® Communication Manager (CM)	• 250 (CM 8.0 and earlier) • 999 (CM 8.1 and later)	This number also applies if CM controls a combination of G250 Branch Gateway, G350 Branch Gateway, G430 Branch Gateway, and G450 Branch Gateway.
Maximum number of G450 Branch Gateways controlled by S8300 Server	50	This number also applies if S8300 Server controls a combination of G250 Branch Gateway, G350 Branch Gateway, G430 Branch Gateway, and G450 Branch Gateway.
Maximum total number of phones supported by G450 Branch Gateway	450	This number applies if G450 Branch Gateway MGC is installed on S8300 as an ICC. Otherwise, the capacity is greater.
Maximum number of IP phones supported by G450 Branch Gateway	450	This number applies if G450 Branch Gateway MGC is installed on S8300 as an ICC. Otherwise, the capacity is greater.
Maximum number of analog phones supported by G450 Branch Gateway	192	–
Maximum number of DCP phones supported by G450 Branch Gateway	192	–
Maximum number of BRI endpoints supported by G450 Branch Gateway	128	–
Simultaneous two-way connections with TDM transcoding from IP phone to a legacy phone or trunk	206	–
Simultaneous two-way connections with TDM transcoding from TDM phones to IP phones	206	–
Maximum number of BRI trunks	64	–

Table continues…

Item	Capacity	Description
Maximum number of PSTN trunks	• 184 (T1) • 240 (E1)	For E1 trunks, 240 channels are supported in Tandem mode. 206 channels are supported for IP to PSTN.
Simultaneous fax transmissions	240	Fax transmissions using VoIP resources
Touch-tone recognition (TTR)	64	–
Tone Generation	Unlimited	–
Announcements ports	63 ports for playback 1 for record	–

Note:

G450 Branch Gateway is not vulnerable to the Spectre and Meltdown hardware issue.

S8300 maximum capacities

You can deploy Avaya Aura® Communication Manager Main Small or Avaya Aura® Communication Manager Remote Survivable (LSP) Small on the S8300 card.

For a complete list of capacities about Main Embedded Small and Survivable Remote Embedded Small, see *Avaya Aura® Communication Manager System Capacities Table*.

Chapter 8: Supported Avaya phones

Branch Gateway supports various Avaya phones, including IP, DCP digital, and analog phones.

IP phones

G450 Branch Gateway supports all Avaya IP phones, including Avaya 1602, 1608, and 1616 H.323 IP phones.

DCP digital phones

Branch Gateway supports the following DCP phones:

- Avaya 1408 DCP Telephone
- Avaya 1416 DCP Telephone
- Avaya 2402 Digital Telephone
- Avaya 2410 Digital Telephone
- Avaya 2420 Digital Telephone
- Avaya 2490 DCP Speakphone
- Avaya 6402 and Avaya 6402D Digital Telephones
- Avaya 6408+ and Avaya 6408D+ Digital Telephones
- Avaya 6416D+ and 6416D+M Digital Telephones
- Avaya 6424D+ and 6424D+M Digital Telephones
- Avaya 75xx and 8510T ISDN BRI endpoints
- Avaya 8403 Digital Telephone
- Avaya 8405B and Avaya 8405D+ Digital Telephones
- Avaya 8410 and 8410D Digital Telephone
- Avaya 8411D Digital Telephone
- Avaya 8434DX Digital Telephone

- IP softphones configured as a Road Warrior and Takeover DCP station
- Definity Extender for an analog endpoint
- Definity Extender for an ISDN endpoint 302 Series Attendant Console
- Avaya 603E Call Master III
- Avaya 603F Call Master IV
- Avaya 607A Call Master V
- Avaya 606B1 Call Master VI
- Avaya eConsole R1 (PC Console R3 with a 8411 digital phone)
- Avaya IP eConsole
- Avaya 9404 DCP Telephone
- Avaya 9408 DCP Telephone

Analog phones

Branch Gateway supports the following Avaya analog phones:

- Avaya 6210 Analog Telephone
- Avaya 6211 Analog Telephone
- Avaya 6218 Analog Telephone
- Avaya 6219 Analog Telephone
- Avaya 6220 Analog Telephone
- Avaya 6221 Analog Telephone

Chapter 9: Technical specifications

Branch Gateway technical specifications include physical dimensions and tolerances, power cord and media module specifications.

Specifications

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

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 the basic configuration, including the mainboard, power supply unit, fan tray, one DSP, and blank panels on media module slots	31 pounds (14 kg)
Ambient working temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10 to 90% relative humidity, non-condensing
Storage temperature	-40°F to 150°F (–40°C to 66°C)
Storage relative humidity	10 to 90% relative humidity, non-condensing
Left air inlet	Up to 104°F (40°C)
Operation altitude	Up to 10,000 ft (3000 m)
Front clearance	2 in. (5 cm)
Rear clearance	4 in. (10 cm)
Side clearance	3 in. (7.6 cm)
AC voltage	90–264 VAC, 47–63 Hz
DC voltage	-48 VDC nom. (-43 VDC to -57 VDC)
Power rating	1780 BTU/h (522 W)
Max AC	7 A
Max DC	13.6 A

Power cord specifications

In North America

The cord set must be UL-listed or CSA-certified, 16 AWG, 3-conductor with a third-wire ground, type SJT. One end must terminate at IEC 60320, a sheet C13 type connector rated 10A, 250 V. The other end must terminate at a NEMA 5-15P attachment plug for nominal 125 V applications or a NEMA 6-15P attachment plug for nominal 250 V applications.

Outside North America

The cord must be VDE-certified or Harmonized (HAR), rated 250 V, 3-conductor with a third-wire ground, 1.0 mm^2 minimum conductor size. At one end, the cord must terminate at a VDE-certified or CE-marked IEC 60320, a sheet C13 type connector rated 10A, 250 V. At the other end, it must terminate at a 3-conductor grounding type attachment plug rated at minimum 10A, 250 V and a configuration specific for the region or country where it is used. The attachment plug must bear the safety agency certifications marks for the region or country where it is installed.

Media module specifications

Description	Value
Height	0.79 in (2 cm)
Width	6.69 in (17 cm)
Depth	12.20 in (31 cm)
Weight	0.7–0.9 lb (300-400 grams)

DC power cord specifications

For DC power, use Avaya DC power cord, material code 700406358.

Chapter 10: Resources

Branch Gateway documentation

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

Title	Description	Audience
Installing and implementing		
Quick Start for Hardware Installation: Avaya G450 Branch Gateway	Describes how to install G450 Branch Gateway in the basic configuration.	Solution architects, implementation engineers, and support personnel
Deploying and Upgrading Avaya G450 Branch Gateway	Describes how to install and upgrade G450 Branch Gateway, perform basic configuration tasks, insert media modules, and connect external devices.	Solution architects, implementation engineers, and support personnel
Administering		
Administering Avaya G450 Branch Gateway	Describes how to configure and manage G450 Branch Gateway after the installation. Contains the detailed information about G450 Branch Gateway features and their implementation.	Solution architects, implementation engineers, and support personnel
Avaya Branch Gateway G450 CLI Reference	Describes the CLI commands for G450 Branch Gateway configuration.	Solution architects, implementation engineers, and support personnel
Avaya Aura® G450 Data Privacy Guidelines	Describes how to administer G450 Branch Gateway to fulfill Data Privacy requirements.	Solution architects, implementation engineers, and support personnel

Finding documents on the Avaya Support website

Procedure

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

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

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

Accessing the port matrix document

Procedure

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

   The list displays the product-specific Port Matrix document.
10. Press **Enter**.

Avaya Documentation Center navigation

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

Important:

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

Using the Avaya Documentation Center, you can:

- Search for keywords.

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

- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

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

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

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

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

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

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

Training

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

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

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Index

Special Characters

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

V

W