Avaya G450 Branch Gateway Overview and Specification

Release 7.1.3
Issue 2
May 2018

© 2010-2018, Avaya Inc.
All Rights Reserved.

Notice

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, 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.

Licenses

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

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

License types

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Product Safety Standards

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

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

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

For a Class B digital device or peripheral:

Note:

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

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

Equipment With Direct Inward Dialing ("DID"):

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

Proper Answer Supervision is when:

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

Permissible exceptions are:

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

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

Automatic Dialers:

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

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

Toll Restriction and least Cost Routing Equipment:

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

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

For equipment approved prior to July 23, 2001:

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

For equipment approved after July 23, 2001:

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

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone

line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

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

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

Means of Connection:

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

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

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

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

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

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

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

Installation and Repairs

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

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

FCC Part 68 Supplier's Declarations of Conformity

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

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

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

Canadian Conformity Information

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

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

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

European Union Declarations of Conformity

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

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

European Union Battery Directive

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

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

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

If this is a Class A device:

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

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

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: 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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: 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 ... 9
Purpose ... 9
Change history ... 9
Chapter 2: G450 Branch Gateway overview ... 10
Avaya Branch Gateway G450 ... 10
Branch Gateway functions ... 10
Branch Gateway specifications ... 11
Minimum firmware requirements for G450 ... 11
Branch Gateway features ... 13
G450 physical description ... 16
Chapter 3: New in this release ... 18
New in Branch Gateway Release 7.1.2 ... 18
New in Branch Gateway Release 7.1 ... 18
Chapter 4: Optional components ... 20
Optional components ... 20
Supported media modules ... 20
S8300D Server hardware requirements ... 21
S8300D Server components ... 21
S8300D Server configuration ... 21
S8300D Server software ... 21
S8300E Server hardware requirements ... 22
S8300E Server components ... 22
S8300E Server configuration ... 22
S8300E Server software ... 23
Telephony media modules ... 23
WAN media modules ... 29
VOIP Modules in G450 ... 30
Media module slot configurations ... 31
Chapter 5: Summary of services ... 33
Summary of services ... 33
IPv6 ... 33
Branch Gateway services ... 34
Physical media ... 35
Media Gateway Controllers ... 36
Audio and Video features ... 39
Additional features ... 42
LAN services ... 43
LAN physical media ... 43
VLANs ... 43

Rapid Spanning Tree Protocol (RSTP)..... 43
Port mirroring..... 43
Port redundancy..... 44
Link Layer Discovery Protocol (LLDP)..... 44
WAN services..... 44
WAN physical media..... 44
WAN features..... 45
Data and Routing features..... 47
Chapter 6: Management, Security, Alarms and Troubleshooting..... 48
Management, Security, Alarms and Troubleshooting..... 48
Management applications..... 48
Management access security features..... 49
Network security features..... 49
Alarms and troubleshooting features..... 50
Chapter 7: Branch Gateway capacities..... 52
Branch Gateway capacities..... 52
G450 maximum Branch Gateway capacities..... 52
S8300 maximum capacities..... 53
Chapter 8: Supported Avaya telephones..... 55
Supported Avaya telephones..... 55
Avaya IP telephones..... 55
Avaya DCP digital telephones..... 55
Avaya analog telephones..... 56
Chapter 9: Technical specifications..... 57
Specifications..... 57
Power cord specifications..... 58
Media module specifications..... 58
Chapter 10: Related resources..... 59
Documentation..... 59
Finding documents on the Avaya Support website..... 60
Training..... 60
Viewing Avaya Mentor videos..... 60
Support..... 61
Using the Avaya InSite Knowledge Base..... 61

Chapter 1: Introduction

Purpose

This document describes tested characteristics and capabilities of Branch Gateway, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.

This document is intended for anyone who wants to gain a high-level understanding of Branch Gateway features, functions, capacities, and limitations within the context of solutions and verified reference configurations.

Change history

The following changes have been made to this document since the last issue:

Issue	Date	Summary of changes
2	December 2017	For 7.1.2, added the section New in Branch Gateway Release 7.1.2 on page 18.
1	May 2016	• Merged the Purpose and Intended Audience sections per GIS Content Evolution Updated Document Standards. • Heading name for this section renamed from *Document changes since last issue* to *Change history*. • Updated the *Training* reference library under the heading *Related Resources*.

Chapter 2: G450 Branch Gateway overview

Avaya Branch Gateway G450

The Avaya Branch Gateway G450 is a multipurpose gateway that can be deployed in medium to large sized branch locations or in wiring-closets servicing buildings and floors, in a campus environment.

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

Branch Gateway functions

The Branch Gateway:

- Works in conjunction with Avaya Aura® Communication Manager IP telephony software running on Avaya Servers to help deliver intelligent communications to enterprises of all sizes
- Combines telephone exchange and data networking, by providing PSTN toll bypass, and routing data and VoIP traffic over the WAN
- Features a VoIP engine, an optional WAN router, and Ethernet LAN connectivity.
- Provides full support for Avaya IP and digital telephones, as well as analog devices such as modems, fax machines, and telephones.

Telephone services on a Branch Gateway are controlled by an Avaya Server operating either as an External Call Controller (ECC) or as an Internal Call Controller (ICC). The Branch Gateway supports:

- The Avaya S8300 Server as an ICC, or as an ECC when the S8300 is installed in another Branch Gateway

An ICC can be used in addition to an ECC with the ICC installed as a Survivable Remote Server (SRS) designed to take over call control in the event that the ECC fails or the WAN link between the branch office and main location breaks. The SRS provides full featured telephone service survivability for the branch office. The Branch Gateway also features Standard Local Survivability (SLS) (IPv4 only), which provides basic telephone services in the event that the connection with the primary ECC is lost.

Branch Gateway specifications

The G450 is a scalable device with a basic configuration consisting of one power supply unit (PSU) and 256 MB RAM, and a single DSP childboard supporting either 20, 80, or 160 VoIP channels. This configuration can be enhanced by adding a redundant PSU, increasing RAM to 512 MB, and up to three additional DSP childboards, increasing the number of VoIP channels to 320 channels. You can also add an external compact flash, increasing the number of announcement files to 1024.

The Branch Gateway is a modular device, adaptable to support different combinations of endpoint devices. While fixed front panel ports support the connection of external LAN switches, network data ports, Ethernet WAN lines, and external routers, eight slots are provided for plugging in optional media modules. Pluggable media modules provide interfaces for different types of telephones, trunks, and WAN links. A combination is selected to suit the needs of the branch. A range of telephony modules provides full support for legacy equipment such as analog and digital telephones. IP phones are supported via an external LAN switch.

The G450 chassis features field replaceable RAM, external compact flash, DSPs, PSUs, fan tray, and main board module for enhanced reliability.

Minimum firmware requirements for G450

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

Table continues…

Firmware version	Build	v1a	v2b	v2d	v3b	Recommended CM Version
						AA 6.2 FP 2, CM 6.3 & CM 5.2.1 SP 16+
BGW 6.3.6 JITC	36.x.y	Yes	Yes	Yes	Yes	AA 6.2 FP 4, CM 6.3.6 AA 6.2 FP3, CM 6.3.2 & CM 5.2.1 SP 16+
BGW 6.3.7+	36.16.0+	Yes	Yes	Yes	MP120 Support	AA 6.2 FP 4, CM 6.3.6+
BGW 6.3.14	36.18.0	Yes	Yes	Yes	Yes	CM 6.3.x,AA 7.0
BGW 7.0	37.20.0	Yes	Yes	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	Yes	Yes	AA 7.0, CM 7.0 AA 6.2 FP 4, CM 6.3.6 +
BGW 7.0.0.2	37.21.0	Yes	Yes	Yes	Yes	AA 7.0, CM 7.0 AA 6.2 FP 4, CM 6.3.6 +
BGW 7.0.1	37.38.0	Yes	Yes	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 7.0.1.1	37.39.0	Yes	Yes	Yes	Yes	AA 7.0, CM 7.0
BGW 7.0.1.2	37.41.0	Yes	Yes	Yes	Yes	AA 7.0 FP 1
BGW 7.1.0+	38.16.0+	Yes	Yes	Yes	Yes	AA 7.0 FP 1, CM 7.0.1 AA 7.0 FP 1, CM 7.0.1 AA 7.0, CM 7.0 + AA 6.2 FP 4, CM 6.3.6 + AA 7.1, CM 6.3.x, AA 7.0 **Note:** The gateways require a 7.x load (37+) to successfully upgrade to load 38.8.0 or newer. Older loads will fail with a failure type `Invalid file`. If the gateway is running 36.x or older load, upgrade to 37.xx before trying to upgrade to 38.xx.
BGW 7.1.2	39.x.y	Yes	Yes	Yes	Yes	AA 7.0 FP 1, CM 7.0.1

Table continues…

Firmware version	Build	v1a	v2b	v2d	v3b	Recommended CM Version
						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 **Note:** The gateways require a 7.1.0.2 load (38.21.0) to successfully upgrade to load 39.5.0 or newer. Older loads will fail with a failure type `Invalid file`. If the gateway is running 38.20.0 or older load, upgrade to 38.21.0 before trying to upgrade to 39.xx.

Branch Gateway features

Some features are supported only in IPv4 as indicated in the following table that summarizes the Branch Gateway features.

Feature type	Description
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
Voice features	• H.248 gateway

Table continues…

Feature type	Description
	• Voice line interfaces: - IP phones - Analog phones - Avaya DCP phones - BRI Phones - FXS/Fax - VoIP - Fax and modem over IP • Voice trunk interfaces: - FXO - 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 • Custom tone detection and generation
Routing and WAN features	**Note:** IPv6 is not supported on the WAN. • Two WAN 10/100 Ethernet ports with traffic shaping capabilities • T1/E1 and USP interfaces • PPPoE (IPv4 only), Frame-relay, and PPP (IPv4 only) • Routing Protocols: Static, OSPF, RIP

Table continues…

Feature type	Description
	• 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 • 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 • Embedded Web Manager (IPv4 only) • RADIUS Authentication support (IPv4 only)

Table continues…

Feature type	Description
	• SNMPv1 traps and SNMPv3 notifications • Telnet (IPv4 only) and SSHv2 support • SCP, TFTP, and FTP clients • Syslog client • Modem access for remote administration • Packet Sniffing • RTP-MIB • Backup and Restore on USB Flash drive

G450 physical description

The G450 Branch Gateway has three hardware versions, referred to as *G450 1.x* , G450 2.x, and *G450 3.x*. The versions 1.x, 2.x, and 3.x refer to the hardware suffix of the G450, which is printed on the label displayed on the rear of the chassis.

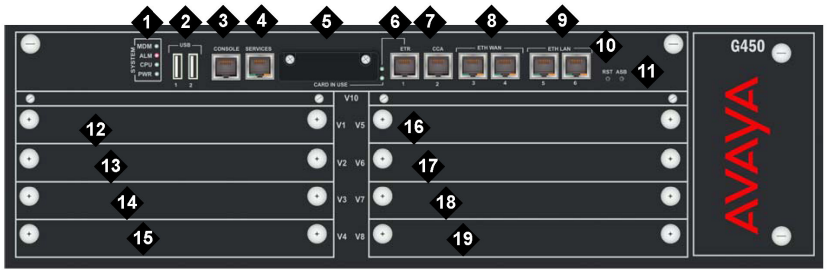

Figure 1: The Branch Gateway G450 1.x Chassis

No	Name	Description
1	System LEDs	LEDs that indicate status of the system
2	USB	USB ports for the system
3	CONSOLE	RS-232 port for services and maintenance access. RJ-45 connector.
4	SERVICES	Ethernet 10/100 port for services and maintenance access. RJ-45 connector.
5	CARD IN USE	Compact flash slot
6	ETR	Emergency Transfer Relay port. 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.

Table continues…

No	Name	Description
9	ETH LAN	Two 10/100/1000 Base TX Ethernet LAN ports. RJ-45 connectors.
10	RST	Reset button. Resets chassis configuration.
11	ASB	Alternate Software Bank button. Reboots the G450 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	Standard media module slot.
17	V6	Standard media module slot.
18	V7	Standard media module slot.
19	V8	Standard media module slot.

For information about the different media modules that can be housed in the G450 media module slots, see Chapter 2: Optional components on page 20.

Chapter 3: New in this release

New in Branch Gateway Release 7.1.2

The following new features and enhancements are available in Branch Gateway 7.1.2.

Enhanced Access Security Gateway (EASG) support

Branch Gateway Release 7.1.2 now supports Enhanced Access Security Gateway (EASG). EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Logins to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

EASG users

EASG access is permitted to five user accounts: init, inads, sroot, craft, and rasaccess.

EASG Product certificate

The EASG Product certificate is embedded in gateway firmware. You can modify or replace the product certificate only through the new software deployment or through patch installation. Using the Branch Gateway CLI, you can view the EASG product certificate information.

New in Branch Gateway Release 7.1

The following new features and enhancements are available in Branch Gateway 7.1.

Password change on first login

Branch Gateway now prompts the user to change the password on the first login attempt.

Notification message for a failed login

Branch Gateway now displays a notification message to a user who makes a failed login attempt.

CLI Support for Secure Shell (SSH)

Branch Gateway CLI now allows the user to configure a set of ciphers, key exchange algorithms and MACs for SSH.

Subject Alternate Name Validation for TLS

When enabled, this new TLS certificate validation option checks that the Subject Alternate Name field of the Root CA certificate matches the address of Communication Manager.

TLS version selection

This new feature specifies what TLS versions are offered by the gateway when connecting to a server.

Certificate Revocation Validation

Increased control over the degree of revocation validation that will performed when validating TLS Certificates.

FIPS Mode Security

Ability to enable FIPS mode security.

Chapter 4: Optional components

Optional components

The Branch Gateway is a versatile device with powerful capabilities. To implement the various services that are supported, a variety of swappable internal components called media modules are available.

Supported media modules

Table 1: Supported media modules

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 (discontinued)	
MM340	1 E1/T1 data WAN port
MM342	1 universal serial data WAN port

S8300D Server hardware requirements

The hardware for S8300D Server as a primary controller is identical to the hardware for S8300D Server as a survivable remote server. The difference between the two configurations is only in software.

S8300D Server components

For a list of S8300D components used in each S8300D configuration, see the S8300D Server configuration section.

S8300D Server configuration

The S8300D Server is supported by Communication Manager Release 5.2 and later.

An S8300D Server is an Intel Core 2 Duo U5700 processor that runs on the Linux operating system. The S8300D Server resides in Slot V1 of a gateway and includes:

- 250-GB hard disk
- 8-GB DRAM (with one 1 GB DIMM)
- 4-GB Internal Solid State Drive (SSD)
- One USB ports and a 10/100 Base-T port
  - One USB port supports a readable DVD/CD-ROM drive, which is used for system installations and upgrades.
- One services port

S8300D Server software

S8300D Server supports the following:

- A web server that is used for:
  - Backing up and restoring customer data
  - Viewing current alarms
  - Maintaining the server
  - Starting and stopping the FTP server
  - Viewing the software license
  - Accessing SNMP to configure trap destinations and to start and stop the master agent

  - Viewing the configuration information
  - Upgrading
- A Linux operating system
- Trivial File Transfer Protocol (TFTP)
- A secure HTTP server for IP phone file downloads
- H.248 Branch Gateway Signaling Protocol
- Control messages over H.323 Signaling Protocol

S8300E Server hardware requirements

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 software.

S8300E Server components

For a list of S8300E components used in each S8300E configuration, see the S8300E Server configuration section.

S8300E Server configuration

The S8300E server is supported by Communication Manager Release 6.0.1 and later.

An S8300E server is an dual core Intel Ivy Bridge processor.

The S8300E server resides in Slot V1 of a gateway and includes:

- 320–GB hard disk
- Two 8-GB of DDR3 SDRAM
- 512-KB L2 cache and 4-MB L3 cache
- Three USB 2.0 ports
- External Ethernet LAN port
- USB port for DVD Drive
- One services Ethernet port

S8300E Server software

S8300E server supports the following:

- A web server that is used for:
  - Backing up and restoring customer data
  - Viewing current alarms
  - Maintaining the server
  - Starting and stopping the FTP server
  - Viewing the software license
  - Accessing SNMP to configure trap destinations and to start and stop the master agent
  - Viewing the configuration information
  - Upgrading
- Linux operating system
- Trivial File Transfer Protocol (TFTP)
- Secure HTTP server for IP phone file downloads
- H.248 branch gateway signaling protocol
- Control messages over H.323 and SIP signaling protocol

Telephony media modules

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

MM711 analog media module

The MM711 provides analog trunk and telephone features and functionality.

MM711 ports

The administrator can configure any of the eight ports of the MM711 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 the PSTN
- MF signaling is supported for CAMA ports
- Analog, tip/ring devices, such as single-line telephones with or without LED message waiting indication

Other MM711 features and functionality

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

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

  Note:

  The Branch Gateway achieves this number of ports by staggering the 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

Figure 2: The MM711 media module

MM714 analog media module

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

Note:

The four analog trunk ports *cannot* be used for analog DID trunks. Instead, the four analog telephone ports must be used.

MM714 ports

The MM714 provides you with the capability to configure any of the four trunk ports as:

- 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 the PSTN. MF signaling is supported for CAMA ports.

MM714 line ports

The MM714 provides you with the capability to configure any of the four telephone ports as:

- A wink-start or an immediate-start DID trunk
- Analog tip/ring devices such as single-line telephones with or without LED message waiting indication

Other MM714 features and functionality

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

  At .1 or less ringer loads, the supported loop length is 20,000 feet (6096 meters) with 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

Figure 3: The MM714 media module

MM714B analog media module

The MM714B analog media module provides all the features provided by the MM714 (see MM714 analog media module on page 24), and in addition provides an emergency transfer relay.

MM714B and ETR

In the event of system failure, the MM714B provides emergency transfer relay (ETR) services by connecting trunk port 5 and line port 4.

Figure 4: The MM714B media module

MM716 analog media module

The MM716 provides 24 analog ports supporting telephones, modem, and fax. These ports can also be configured as DID trunks with either wink-start or immediate-start. The 24 ports are provided via a 25 pair RJ21X amphenol connector, which can be connected by an amphenol cable to a breakout box or punch-down block.

MM716 ports

The MM716 provides you with the capability to configure any of the 24 ports as:

- Analog tip/ring devices such as single-line telephones with or without LED message waiting indication
- A wink-start or an immediate-start DID trunk

Other MM716 features and functionality

- Three ringer loads, which is the Ringer Equivalency Number (REN), for the following loop lengths for all 24 ports.
  - 20,000 feet (6096 meters) with 0.65 mm wire
  - 16,000 feet (4877 meters) with 0.5 mm wire
  - 10,000 feet (3048 meters) with 0.4 mm wire

  At .1 or less ringer loads, the supported loop length is 20,000 feet (6096 meters) with 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 is compatible with Avaya Aura® Communication Manager release 3.1 and higher, and Branch Gateway firmware version 29.x.x and higher.

Figure 5: The MM716 media module

MM712 DCP media module

The MM712 DCP media module provides eight DCP telephone ports. The ports support two-wire Digital Communications Protocol (DCP) telephones. See Supported Avaya telephones on page 55 for a list of compatible DCP telephones.

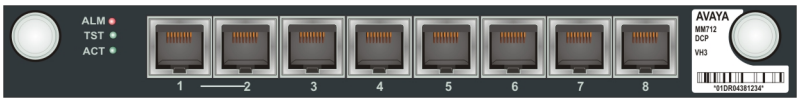

Figure 6: The MM712 media module

MM717 DCP media module

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 via a standard amphenol cable to a punch-down block with RJ-11 jacks. The MM717 allows you to use one of the smaller media module slots for a large number of DCP telephones.

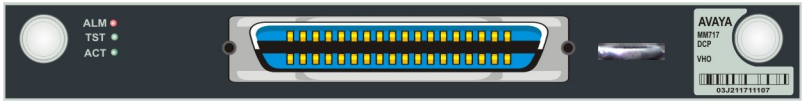

Figure 7: The MM717 media module

MM710B E1/T1 media module

Note:

This information applies to the MM710 as well.

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

The MM710B 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

Figure 8: The MM710B media module

MM720 BRI media module

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

Note:

The MM720 BRI media module cannot be administered 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. Communication Manager 3.1 enables combining B-channels, using BONDing, to form a higher bandwidth connection. Finally, if the MM720 BRI Media Module is administered to support BRI endpoints, it cannot be used 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. Information is communicated in two ways:

- Over two 64-kbps channels, called B1 and B2, that can be circuit-switched simultaneously
- Over a 16-kbps channel, called the D-channel, that is used for signaling. The MM720 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 when in the 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 the BRI endpoints.

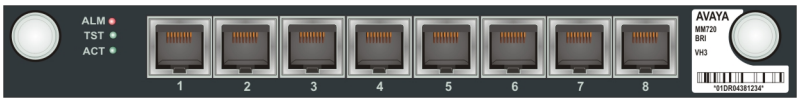

Figure 9: The MM720 media module

MM721 BRI media module overview

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

Note:

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 for just stations or just 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 the BRI endpoints.

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

The MM721 BRI media module communicates information in two 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 that is used for signaling

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

The MM721 supports the G450 and G430 Branch Gateways with Communication Manager Release 6.0.1 build 31_18_1.

The MM721 is supported by Communication Manager release 6.0.1 and later and Gateway firmware version 31.18.1 and later.

Note:

If you replace the MM720 media module, first uninstall the MM720 media module before installing the MM721 media module.

The following table provides the MM721 media module display information on different Communication Manager releases.

Release	5.2.1/6.0.1 and earlier	5.2.1 SP7/6.0.1 SP1	6.2 and later
Administer	MM720 (non-native admin)	MM720 (non-native admin)	MM721 (Native)
Insert	MM721	MM721	MM721
Result	No Board	MM720X	MM721

Front panel of the MM721 media module

MM722 BRI media module

The MM722 BRI media module provides two 4 wire S/T ISDN BRI 2B+D access ports with RJ-45 jacks. Each port interfaces to the central office at the ISDN T reference point. Information is communicated in the same manner as for the MM720. See MM720 BRI media module on page 27.

Figure 10: The MM722 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

The Branch Gateway supports the MM340 E1/T1 WAN and MM342 Universal Serial Port WAN media modules.

MM340 E1/T1 WAN media module

Note:

The MM340 is no longer sold.

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

Figure 11: The MM340 media module

MM342 universal serial data WAN media module

Note:

The MM342 is no longer sold.

The MM342 media module provides one universal serial data WAN access port. The MM342 supports the following WAN protocols:

- V.35/ RS449
- X.21

Required cable

For these connections, one of the following cables is required:

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

Figure 12: The MM342 media module

VOIP Modules in G450

A media processor or a VOIP module provides the resources/channels to support a voice call.

A G450 has four VOIP slots. It supports the VOIP modules listed in the table below:

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	The MP160 is capable of supporting new media services such as V.150.1 and Opus codec. In the past, all DSP cards were capable of supporting all codec types, albeit with various performance differences in terms of point costs. However, the V. 150.1 protocol is not supported on the older VOIP modules. MP160 supports a maximum of 160 channels. Supports a maximum of 80 channels with the Opus codec.

Configuration matrix

A G450 can support MP20 and MP80 in any configuration for the 4 slots. G450 supports a maximum of 320 channels.

The following are permitted combinations of optional VoIP (MP) modules on G450 Branch Gateway only.

Combination of Cards	MP80 Card	MP20 Card	MP160 Card
Combination # 1	-	-	2
Combination # 2	-	2	1
Combination # 3	2	-	1
Combination # 4	1	1	1

Note:

Once the installation for MP160 is determined, the MP80/20s can be installed in any of the remaining slots.

Media module slot configurations

When choosing a combination of media modules to install in the Branch Gateway chassis, consider the slots in which each module type can be housed, and the limitations and recommendations regarding combinations of media modules.

Permitted slots

The Branch Gateway G450 chassis has eight media module slots, marked V1, V2, V3, V4, V5, V6, V7, and V8. Each media module is restricted to certain slots.

Table 2: Permitted slots for media modules

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 media module capacity

The G450 chassis is designed to accommodate:

- Up to eight telephony media modules (MM710, MM711, MM712, MM714, MM714B, MM716, MM717, MM720, MM722)
- Up to three WAN media modules (MM340, MM342)
- Up to one S8300 server

Chapter 5: Summary of services

Summary of services

The Branch Gateway offers various services, which are described in Branch Gateway services on page 34 , LAN services on page 43 and WAN services on page 44.

IPv6

Internet Protocol version 6 (IPv6) is the successor to IPv4. IPv6 supports 128–bit addresses and satisfies the rapidly growing demand for IP addresses. In contrast, IPv4 supported 32–bit. IPv6 also improves security, ease of configuration, and routing performance. IPv6 can coexist with IPv4 networks, easing the transition process.

The IETF (Internet Engineering Task Force) published RFC 2460, the internet standard specification that defines IPv6, in December 1998.

Addressing

By using 128-bit addresses, IPv6 has about $3.4x10^{38}$ unique IP addresses, more than enough for every network device. This eliminates the IPv4 mechanisms, such as NAT (network address transitions), 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.

Simplicity

IPv6 simplifies the routing process by changing the packet header and packet forwarding:

- 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 no longer need to calculate the time a packet spent in a queue.
- IPv6 supports stateless address configuration, so 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 ease the deployment of IPv6 running alongside IPv4. The key to the transition is dual-stack hosts. Dual-stack hosts refers 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 a Hybrid. The Hybrid is the common form on recent server operating systems and computers.

When an IPv6 host or network must use the existing IPv4 infrastructure to carry IPv6 packets, *Tunneling* provides the solution. Tunneling encapsulates IPv6 packets within IPv4. Tunneling can be either *automatic* or *configured*, the latter being more suitable for large, well-administered networks.

Key differences between IPv4 and IPv6

Parameter	IPv4	IPv6
Address space	32-bit, about 4.3×10^9	128-bit, about 3.4×10^{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	No Broadcast. Various forms of Multicast — better network bandwidth efficiency
QoS support	ToS using DIFFServ	Flow labels and flow classes, more granular approach.

Feature Support in Avaya Branch Gateways

Certain Branch Gateway features are not supported in IPv6.

Branch Gateway services

The Branch Gateways provide a telephone exchange service, supporting the connection of various types of telephones and outside telephone lines. Telephones and lines are connected to the Branch Gateways through media modules on the chassis. Different media modules provide access ports for different types of telephones and lines.

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

This section describes the services the Branch Gateway provides as a gateway.

Voice over IP (VoIP)

The Branch Gateway:

- Features up to four VoIP DSPs that provide voice services over IP data networks.

- Allows you to use many types of telephones and trunks that do not directly support VoIP.
- Translates voice and signalling data between VoIP and the system used by the telephones and trunks, as follows: Avaya media modules convert the voice path of traditional circuits such as analog trunk, T1/E1, and DCP to a TDM bus inside the Branch Gateway. The VoIP engine then converts the voice path from the TDM bus to a compressed or uncompressed and packetized VoIP on an Ethernet connection.

The Branch Gateway provides VoIP services over the LAN and WAN. The G450 supports up to four VoIP DSP childboards. The maximum number of active channels supported is 105.All channels can be bi-directional FAX, G.711 u/A, G.726A calls, in case of G.729A/AB the maximum number of channels on the on-board DSP is 20.

Physical media

There are various types of telephones and lines supported by the Branch Gateway and access ports provided for their connection.

Telephones

The Branch Gateway supports IP telephones, Avaya DCP telephones, analog telephones, and BRI telephones. For information about which Avaya telephones are supported, see Appendix B: Supported Avaya telephones on page 55.

Telephones must be connected to the correct type of port for the telephone type. Different types of telephone ports are provided by different media modules. The table below lists which ports you can use to connect each type of telephone. See Chapter 2: Optional components on page 20 for more information about each type of port and media module.

Table 3: Telephones supported and ports provided

Telephone type	Ports
IP telephones and softphones	An external LAN switch must be connected to one of the front panel ETH LAN ports. **Note:** The registration and signaling control information is under the direct control of the Avaya Aura® Communication Manager server.
Avaya DCP digital telephones	DCP ports on the MM712 and MM717 media modules.
Analog telephones	Analog line ports on the MM711, MM714, MM714B, and MM716 analog media modules.

Outside telephone lines

The table below lists which modules you can use to connect each type of outside line. See Chapter 2: Optional components on page 20 for more information about each type of port and media module.

Table 4: Outside telephone lines supported and ports provided

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 analog media module. Universal analog ports on MM711. DID trunk ports with wink-start and immediate-start only on MM716.
T1/E1 voice lines	The T1/E1 port on the MM710 T1/E1 media module.

Media Gateway Controllers

A Media Gateway Controller (MGC) controls telephone services on a Branch Gateway. An MGC may be internal or external to the Branch Gateway. An Internal Call Controller (ICC) is an internal MGC. An External Call Controller (ECC) is an external MGC that communicates with the Branch Gateway over the network.

An Avaya server managed with Avaya Aura® Communication Manager (Communication Manager) software acts as an MGC for the Branch Gateway.

Supported Avaya servers

The MGCs supported by the Branch Gateway include both ECCs and ICCs. The Branch Gateway supports the following MGCs:

Table 5: MGCs supported by the Branch Gateways

MGCs	Type	Usage
Avaya S8300E Server	Media module	ICC, ECC or LSP
Avaya S8300D Server	Media module	ICC, ECC or LSP
Avaya S8800 Server	External	ECC
Dell™ PowerEdge™ R610 Dell™ PowerEdge™ R620 Dell™ PowerEdge™ R630	External	ECC
HP ProLiant DL360 G7 HP ProLiant DL360 G8 HP ProLiant DL360 G9	External	ECC

Configuration rules for Branch Gateway options

The Branch Gateway provides the following configuration options to help you ensure continuous telephone services:

- You can configure the Media Gateway to use up to four MGCs. Each controller can be configured with one IPv4 and/or one IPv6 address. Each address configured is either the

IPv4 address of a TN799 (C-LAN) board connected to the server or the IPv4/IPv6 address of the Processor Ethernet interface of Avaya Aura® Communication Manager. The four addresses are grouped into primary and secondary controllers, using the transition point to separate the two groups.

- Using the connection preserving migration feature, you can configure the Branch Gateway to preserve the bearer paths of stable calls if the Branch Gateway migrates to another MGC (including an SRS), including migration back from an SRS to the primary MGC. A call for which the talk path between parties in the call is established is considered stable. A call consisting of a user listening to announcements or music is not considered stable and is not preserved. Any change of state in the call prevents the call from being preserved. For example, putting a call on hold during MGC migration causes the call to be dropped. Special features, such as conference and transfer, are not available on preserved calls. Connection preserving migration preserves all types of bearer connects except BRI. PRI trunk connections are preserved.
- You can configure Standard Local Survivability (SLS) to enable a local Branch Gateway to provide a degree of MGC functionality when no link is available to an external MGC. You configure SLS from the Branch Gateway using the 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 telephones, IP softphones, and DCP telephones. SLS is available on IPv4 only
- You can configure Enhanced Local Survivability (ELS) by installing an S8300 in the Branch Gateway as a Survivable Remote Server (SRS). In this configuration, the S8300 is not the primary MGC but takes over to provide continuous telephone service if all external MGCs become unavailable. Calls in progress continue without interruption when the S8300 takes over.
- You can configure the dialer interface to connect to the Branch Gateway's primary MGC by a serial modem if the connection between the Branch Gateway and the MGC is lost.
- You can configure Avaya Communication Manager to support the auto fallback feature, which enables an Branch Gateway being serviced by an SRS to return to the primary MGC automatically when the connection is restored between the Branch Gateway and the MGC. When the Branch Gateway is being served by the SRS, it automatically attempts to register with the MGC at periodic intervals. The MGC can deny registration in cases in which it is overwhelmed with call processing, or in other configurable circumstances. By migrating the Branch Gateway to the MGC automatically, a fragmented network can be unified more quickly, without the need for human intervention.

  Note:

  Auto fallback does not include survivability. Therefore, there is a short period during registration with the MGC during which calls are dropped and service is not available. This problem can be minimized using the connection preserving migration feature.

- The Branch Gateway features a dynamic trap manager that enables you to ensure that the Branch Gateway sends traps directly to the currently active MGC. If the MGC fails, the dynamic trap manager ensures that traps are sent to the backup MGC.

Branch Gateway management

Branch Gateway is managed by Communication Manager Release 7.0.

Communication Manager features

Communication Manager is an open, scalable, highly reliable, and secure telephony application. Communication Manager provides user and system management functionality, intelligent call routing, application integration and extensibility, and enterprise communications networking. Communication Manager offers over 700 features, in the following categories:

- Telephony features
- Localization
- Collaboration
- Mobility
- Messaging
- Telecommuting
- System management
- Reliability
- Security, privacy, and safety
- Hospitality
- Attendant features
- Networking
- Intelligent call routing
- Application programming interfaces

Communication Manager software applications

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

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

Audio and Video features

Branch gateways also provide the following audio and video related features:

Call center capabilities

With large announcement storage including optional compact flash, large voice trunk capacity, and 64 announcement ports for announcement record and playback, the Branch Gateway supports call center features.

Emergency Transfer Relay (ETR)

The Emergency Transfer Relay (ETR) feature provides basic telephone services in the event of a power outage or a failed connection to Communication Manager. ETR services are provided on the MM714B media modules by connecting the module's trunk port 5 to line port 4. You can also optionally connect two external 808A ETR panels to the Branch Gateway. Each 808A Emergency Transfer Panel provides emergency trunk bypass or power-fail transfer for up to five incoming trunk loops to five analog phones and maintains connections on return from emergency transfer mode.

Contact closure

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

Fax, modem, TTY over IP

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

Service Level Agreement Monitor

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

SLA Monitor performs analysis on the following network elements:

- Correct Differentiated Services (DiffServ) issues.
- Handle rogue applications.

- Provide real-time visibility to live sessions.

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

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

G430 Branch Gateway and G450 Branch Gateway act as the SLA Monitor agents.

For more information on the SLA Monitor server and agent, see *Operations Intelligence Suite Advanced Implementation Guide for SLA Mon*.

T.38 Fax with Fallback to G.711 Pass-Through

T.38 Fax with Fallback to G.711 Pass-Through feature provides the functionality to enterprise networks managed by Communication Manager to interoperate with the older Verizon networks that currently 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.

The operation of T.38 Fax with Fallback to G.711 Pass-Through is summarized as follows:

- The call connection is signaled for standard T.38 fax relay.
- In the event of a failure to successfully negotiate T.38 fax relay, Communication Manager issues a re-INVITE to a G.711 mode of operation.
  - With PCM (G.711) codec sampling, there is an effort made to simulate a circuit-switched clear channel transport.
- The fax call is in the G.711 mode until the user disconnects.

Note:

This feature only works 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*, 555-245-205.

T.38 with Error Correction Mode

Prior to Release 6.3, the T.38 Fax feature had no error correction capability. This is a problem for many customers and reduces the overall success rate of large fax transmissions. T.38 with Error Correction Mode (ECM) corrects errors without retransmitting multiple pages.

The operation of T.38 with ECM is summarized as follows:

- Communication Manager instructs the gateway to use ECM as part of the T.38 Fax capabilities exchange if:
  - The local media gateway indicates support for this feature through capability exchange.

  - IP codec set is set to **T.38-standard** .
  - ECM is set to **yes**.
- Fax machines with the memory 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 packets of data.
  - After receiving the 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 the fax machines is disconnected.

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

List Trace and List Measurement

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

The standard List Trace command provides enhanced information for the V.150.1 call state information. The goal is to avoid dependency on Wireshark captures and other logging tools. The List Trace command provides easy to read logging information.

The List Measurement command aggregates the usage for V.150.1 calls and provides this in the summary for 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 Server*, 03-300431.

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 for supporting interoperability with secure third-party terminal devices.

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

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

Benefits of V.150.1 MoIP:

- Can transform analog tone events into digital control messages, so that the protocol can pass over hops.
- Can recover from loss and operate at higher speeds up to V.92 as the protocol is sent in sequenced packets.

- Can interoperate with many different vendors.
- Can eliminate extra trunking because of convergence of data, voice, and fax.

For more information about V.150.1 (MoIP), see *Configuring V.150.1 on the Avaya G450 and G430 Branch Gateway*.

MP160 DSP daughter board

To support the V.150.1 Modem over IP feature on the G450 Branch Gateway, a new DSP card MP160 is introduced in Release 6.3. MP160 supports up to 160 VoIP channels on the G450 Branch Gateway. MP160 is used for V 150.1 and non V 150.1 calls on the G450 Branch Gateway. The G450 supports mixed DSP boards of different DSP channel capacities. The DSP channel count on G450 Branch Gateway must not exceed 320.

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

Additional features

H.248 Registration Source Port

You can define the source port range that the gateway uses when registering with Communication Manager by 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 a range, the gateway selects a port within the default range of 1024 to 65535.

For more information about the CLI commands, see *CLI Reference Avaya Branch Gateway G450*, 03-602056.

Accessing diagnostic logs

With the following CLI commands, you can obtain diagnostic logs.

- **`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 CLI commands, see *Administering Avaya G450 Branch Gateway*, 03-603234 and *CLI Reference Avaya Branch Gateway G450*, 03-602056.

LAN services

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

LAN physical media

The 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. The LAN ports are connected to the internal LAN switch and support HP auto-MDIX, which automatically detects and corrects the polarity of crossed cables. This results in simplified LAN installation and maintenance.

VLANs

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

The Branch Gateway G450 supports up to 64 VLANs. The following VLAN features are supported:

- VLAN port grouping. Port VLANs can be used to group LAN ports into logical groups.
- Ingress VLAN Security. You configure a list of ingress VLANs on each port. Any packets tagged with an unlisted VLAN are dropped when received on the port.
- Class of Service (CoS) tagging. Packets are tagged with VLANs per CoS.
- Inter-VLAN routing. You can configure specific VLANs to permit access to the WAN while others can be configured to deny access to the WAN.

Rapid Spanning Tree Protocol (RSTP)

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

Port mirroring

The Branch Gateway supports network traffic monitoring by port mirroring. You can configure port mirroring on any LAN port. You 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 monitor port.

Port redundancy

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

Link Layer Discovery Protocol (LLDP)

LLDP simplifies network troubleshooting and enhances the ability of network management tools to discover and maintain accurate network topologies in multi-vendor environments. LLDP defines a set of advertisement messages (TLVs), a protocol for transmitting the TLVs, and a method for storing the information contained in the received TLVs. This allows stations attached to a LAN to advertise information about the system and about the station's point of attachment to the LAN to other stations attached to the same LAN. These can be reported to the management station via SNMP MIBs.

LLDP is supported on the front panel ETH LAN ports.

WAN services

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

Note:

Certain WAN services are supported on IPv4 only.

WAN physical media

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

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

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

WAN line support

The Branch Gateway supports the following types of data WAN line:

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

Media modules necessary for each WAN line

The table below lists which media modules to install to connect each type of outside WAN line. For more information about each type of media module, see Chapter 2: Optional components on page 20.

Table 6: Outside WAN lines supported and matching media modules

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

WAN features

The Branch Gateway supports the following WAN features:

Note:

These features are only available on IPv4.

- Traffic shaping. The traffic shaping function estimates the parameters of the incoming traffic and takes action if it measures traffic exceeding agreed parameters. The action could be to drop the packets or mark them as being high drop priority.
- PPP over channeled and fractional E1/T1. The Branch Gateway has the ability to map several PPP sessions to a single E1/T1 interface.
- PPP over Universal Serial Port
- PPPoE
- Unframed E1 for enabling full 2.048 Mbps bandwidth usage
- Point-to-Point Frame Relay encapsulation over channelized/fractional/unframed E1/T1 ports or over a Universal Serial Port interface
- Frame Relay LMI types supported: ANSI (Annex D), ITU-T:Q-933 (Annex A0), LMI-Rev1, and 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 WAN bandwidth. When Dynamic CAC is enabled on an interface, the Branch Gateway informs the MGC of the actual bandwidth of the interface and tells the MGC to block calls when the bandwidth is exhausted.
- Quality of Service (QoS). The 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 the real-time response time that is required for VoIP. The Branch Gateway also supports the VoIP Queue and Priority Queue legacy queuing methods.
- Weighted Random Early Detection (WRED). The Branch Gateway uses WRED on its ingress and egress queues to improve the performance of the network when overloaded. The purpose of WRED is to indicate to transmitting hosts to reduce their transmission speed when the ingress Branch Gateway queues are congested.
- Policy. Each interface on the 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 define which packets should be forwarded or denied access to the network. QoS lists change the DSCP and 802.1p priority of routed packets according to the packet characteristics.
- Policy-based routing. The 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 the 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 (Internet Service Providers), and defining backup routes for defined classes of traffic.
- RTP Header Compression. The Branch Gateway saves up to 60% of the bandwidth necessary using RTP compression. It also enhances the efficiency of voice transmission over the network by compressing the headers of Real Time Protocol (RTP) packets, thereby minimizing the overhead and the delays involved in RTP implementation.
- TCP Header Compression. The Branch Gateway uses Transmission Control Protocol (TCP) header compression to reduce the amount of bandwidth needed for non-voice data. TCP header compression can be applied either as part of RTP Header Compression via IPCH, or using the Van Jacobson method defined in RFC 1144.
- Inter-Gateway Alternate Routing (IGAR). The Branch Gateway uses IGAR as a means to use the PSTN as an alternative to the WAN interface under certain definable conditions. In providing an alternate routing mechanism, IGAR preserves the internal makeup of the call so that the call can be successfully terminated to its original internal destination.

Data and Routing features

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

Note:

Features labelled * are only available on IPv4.

- Interfaces*
- Routing table
- VPN
- GRE tunneling*
- DHCP and BOOTP relay*
- DHCP server
- 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

Management, Security, Alarms and Troubleshooting

Management applications

Use any of the following applications to manage the Branch Gateway:

- Command Line Interface
- Branch Gateway Manager and Embedded Web Manager
- Avaya Integrated Management

Branch Gateway Command Line Interface (CLI)

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

You can access the CLI with any of the following:

Note:

Telnet and the Services port are supported on IPv4 only.

- Telnet through the network
- Telnet through dialup, using a dialup PPP network connection

  Note:

  Telnet is disabled by default on the Branch Gateway

- A console device connected to the Console port or Services port on the Branch Gateway front panel
- SSH (Secure Shell), which enables you to establish a secure remote session over the network, Services port, or dial in modem (PPP).
- SSH is enabled by default.

For information about each command in the CLI, see *Avaya Branch Gateway G450 CLI Reference*.

For information about how to use the CLI to perform specific configuration tasks, see *Administration for the Avaya Branch Gateway G450*.

Avaya Branch Gateway Manager and Embedded Web Manager

Note:

Avaya management tools are supported in IPv4 only.

The Avaya Branch Gateway Manager is a web-enabled graphical administration tool for configuring a single Branch Gateway device. You can use the Gxxx Manager to configure the Branch Gateway chassis and media modules. You can also use it for status monitoring and troubleshooting. You can open Avaya Branch Gateway Manager from a web browser on a computer on the same network as the device.

For information about Avaya Branch Gateway Manager, see *Administering Avaya G450 Branch Gateway*.

Management access security features

The Branch Gateway features the following management security mechanisms:

- A basic authentication mechanism in which users are assigned passwords and privilege levels
- Support for user authentication provided by an external RADIUS server
- SNMPv3 user authentication
- Secure data transfer via SSH and SCP with user authentication
- EASG authentication for remote service logins. EASG is a challenge-response authentication method that is more secure than password authentication and does not require a static password.
- Management access can be restricted to an Out of Band Interface, LAN or WAN.

Network security features

The Branch Gateway provides the following network security features:

- Private secure connections can be configured between the Branch Gateway and a remote peer, using VPN (Virtual Private Network). VPN at the IP level is deployed using a standards-based set of protocols defined by the IETF called IPSec. IPSec provides privacy, integrity, and authenticity to information transferred across IP networks.
- Protection against DoS (Denial of Service) attacks via:
  - MSS notifications (IPv4 only). The Branch Gateway identifies predefined or custom-defined traffic patterns as suspected DoS attacks and generates SNMP notifications, referred to as Managed Security Services (MSS) notifications. MSS notifications are intercepted and, if certain conditions are met, may be forwarded to the Avaya Security

Operations Center (SOC) as INADS alarms. The SOC is an Avaya service group that handles DoS alerts, responding as necessary to any DoS attack or related security issue.

- SYN cookies, which protect against a well-known TCP/IP attack in which a malicious attacker targets a vulnerable device and effectively prevents it from establishing new TCP connections.

- From Release 7.0, Branch Gateway supports Transport Layer Security (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 three essential services to all the applications running above it:
  - Encryption
  - Authentication
  - Data integrity
- TLS Certificate validation is now time-zone aware based on the values one has administered in Communication Manager.

Alarms and troubleshooting features

The Branch Gateway has extensive features for error detection, alarms, and troubleshooting. Detailed diagnostic information and troubleshooting are provided by software-based solutions accessible by laptops in the field or remotely from an administrator's computer. *Administration for the Avaya Branch Gateway G450* provides a comprehensive guide to configuring and using these solutions.

Front panel LEDs

LEDs on the front panel of the Branch Gateway and their media modules give a quick overall understanding of the health of the system and subsystems. When alarms or problems occur, LEDs indicate that a technician's attention is needed.

Automatic error detection

During normal operations, software or firmware automatically detects and attempts to fix or circumvent error conditions. Errors are detected in two ways:

- Firmware on a system component during ongoing operations
- A "periodic test" or a "scheduled test" started by software

A technician can run more comprehensive tests on demand.

SNMP

Note:

SNMP is supported on IPv4 only.

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

Packet sniffing

The Branch Gateway features packet sniffing on IPv4 and IPv6. All IP and ARP packets that pass through the Branch Gateway are recorded. The recorded packets are stored in a file that can be uploaded either to the Avaya server or to a PC and read by Ethereal for troubleshooting purposes.

VoIP debugging using RTP-MIB

The Branch Gateway includes the RTP-MIB feature for debugging QoS-related problems across the VoIP network without any dedicated hardware. During each RTP stream, counters representing various QoS metrics increment whenever configured thresholds for the metrics are exceeded. A limited history of the QoS metric statistics is stored on the Branch Gateway for active and terminated RTP streams. Statistics can be displayed via the Branch Gateway CLI. In addition, the Branch Gateway can be configured to send SNMP traps to the SNMP trap manager on the Avaya server at the termination of each RTP stream that has QoS problems. The traps are converted to syslog messages and stored for viewing in the messages file on the Avaya server hard disk.

Chapter 7: Branch Gateway capacities

Branch Gateway capacities

G450 maximum Branch Gateway capacities

Table 7: G450 Branch Gateway capacities

Description	Capacity	Comments
Maximum number of G450 Branch Gateways controlled by an S85XX or S87XX server	250	This number also applies if the same external server controls a combination of Avaya G450, G430, G350, G250, and G700 Branch Gateways.
Maximum number of G450 Branch Gateways controlled by an S8300 server housed in another G450 Branch Gateway.	50	This number also applies if the same external server controls a combination of Avaya G450, G430, G350, G250, and G700 Branch Gateways.
Maximum number of G450 Branch Gateways controlled by an S8300 server housed in a G700 Branch Gateway. **Note:** The G700 is no longer sold.	50	This number also applies if the same external server controls a combination of Avaya G450, G430, G350, G250, and G700 Branch Gateways.
Maximum total number of telephones supported by the G450	450	Assumes that the MGC is an S8300 installed in the G450 as an ICC. Otherwise, the capacity is greater.
Maximum number of IP telephones per G450 Branch Gateway	450	Assumes that the MGC is an S8300 installed in the G450 as an ICC. Otherwise, the capacity is greater.
Maximum number of analog phones per G450 Branch Gateway	192	
Maximum number of DCP phones G450 Branch Gateway	192	

Table continues…

Description	Capacity	Comments
Maximum number of BRI endpoints per G450 Branch Gateway	128	
Simultaneous two-way conversations with TDM transcoding from IP phone to legacy telephone or trunk.	206	
Simultaneous two-way conversations with TDM transcoding from TDM phones to IP phones	206	
Maximum number of BRI trunks	64	
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
Miscellaneous		
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	

S8300 maximum capacities

Table 8: S8300 capacities

Item	Quantity Supported
Number of Users per S8300	2400
Number of Trunks per S8300	2400
Total Endpoints (Trunks and Users) per S8300	900
MGs per S8300	50
LSPs per S8300	49
MGs per LSP	50
Announcement Sources per S8300	50
Busy Hour Calls (Maximum, non-call center)	10,000
Locations	50

For a complete list of capacities, see *Avaya Aura® Communication Manager System Capacities Table*.

Important note regarding Spectre and Meltdown vulnerability and Release 7.1.3:

Note:

The G430/G450 Branch Gateways are not vulnerable to the Spectre and Meltdown hardware issue. The processor used by the G430/G450 Branch Gateways is not included in the list of processors identified to be impacted by the Spectre and Meltdown vulnerabilities.

However, an S8300D installed within the gateway that is upgraded to Release 7.1.3 may be impacted as indicated below.

Note:

The introduction of Spectre and Meltdown fixes with 7.1.3 impacts the S8300D scalability performances. A survivable remote configuration (Communication Manager LSP and Branch Session Manager) with the Spectre and Meltdown fixes enabled can only now support 200 users with up to 500 BHCC traffic.

Since these fixes are enabled by default, consider whether configuration changes are in order to plan an 7.1.3 upgrade.

The following options should be considered if higher capacity is required from the S8300D:

- Disabling the Spectre and Meltdown fixes on the S8300Ds enables the S8300D to deliver the same level of capacity as with 7.1.2 and before.
- If disabling the fixes on the S8300D is not an option, plan to upgrade the embedded server to the latest S8300E model.

For more information about Spectre and Meltdown fixes included in Avaya Aura® Release 7.1.3, see PSN020346u on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101048606.

Chapter 8: Supported Avaya telephones

Supported Avaya telephones

Avaya Branch Gateways support various Avaya telephones, including IP, DCP digital, and analog telephones.

Avaya IP telephones

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

Avaya DCP digital telephones

The DCP media modules supported by the Branch Gateway support the following DCP telephones:

- 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 Telephone
- Avaya 6424D+ and 6424D+M Digital Telephone
- Avaya 75xx and 8510T ISDN BRI endpoints
- Avaya 8403 Digital Telephone
- Avaya 8405B and Avaya 8405D+ Digital Telephones

- Avaya 8410 and 8410D Digital Telephones
- Avaya 8411D Digital Telephone
- Avaya 8434DX Digital Telephone
- IP softphones that are configured as “Road Warrior” and “Take Over” a DCP station
- Definity Extender – Analog single endpoint
- Definity Extender – ISDN single endpoint 302 series Attendant Console (302D)
- 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 8411 digital telephone)
- Avaya IP eConsole
- Avaya 9404 DCP Telephone
- Avaya 9408 DCP Telephone

Avaya analog telephones

The Branch Gateway supports the following Avaya analog telephones:

- 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

Specifications

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

Table 9: Avaya Branch Gateway G450 specifications

Description	Value
Height	5.25 in. (3U, 133.3 mm)
Width	19 in. (482.6 mm)
Depth	18 in. (460 mm)
Weight of empty chassis	16.5 pounds (7.5 kg)
Weight of chassis with basic configuration, including main board, power supply unit, fan tray, one DSP, and blank panels on the media module slots	31 pounds (14 kg)
Ambient working temperature	32° to 104°F (0° to 40°C)
Storage temperature	–40°F to 150°F (–40°C to 66°C)
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)
Humidity	10 to 90% relative humidity, non-condensing
Voltage	90-264 VAC, 47-63 Hz
Power rating	1780 BTU/h (522 W)
Max current	7 A

Power cord specifications

For North America

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

For outside North America

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

Media module specifications

Table 10: Media modules

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)

Chapter 10: Related resources

Documentation

Title	Description	Number
Installation		
Quick Start for Hardware Installation for the Avaya Branch Gateway G450	Describes how to install the Avaya Branch Gateway G450. This document includes content for G450 assembly and basic configuration.	03-602053
Deploying and Upgrading Avaya G450 Branch Gateway	Describes how to install and upgrade G450 , prepare it for software configuration, and perform certain basic configurations. Also describes how to insert media modules and connect external devices to G450 and media module ports.	03-602054
Administration		
Administering Avaya G450 Branch Gateway	Describes how to configure and manage the G450 after installation. Contains detailed information about all the features of G450 and how to implement them.	03-602055
Avaya Branch Gateway G450 CLI Reference	Describes the commands in the G450 CLI.	03-602056
Maintenance		
Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers	Describes MOs and how to resolve alarms.	03-300430
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers	Describes all the commands across platforms.	03-300431
Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers	Describes maintenance procedures such as network recovery.	03-300432

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

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
4U00030E	Knowledge Access: Avaya Aura® Communication Manager and CM Messaging - Embedded Implementation.
4301W	Avaya Unified Communications - Core Components.
7120V	Integration Basics for Avaya Enterprise Team Engagement Solutions (Virtual Instructor Led).
4302W	Avaya Unified Communications - Gateways and Endpoints.

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.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://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.

Related links

Using the Avaya InSite Knowledge Base on page 61

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Support on page 61

Index

Numerics

802.1x 49

A

Access 42
Alarms and troubleshooting 50
analog telephones 56
ASB button 16
Automatic error detection 50
Avaya Aura Communication Manager (Avaya Aura CM)
    server integration 10
Avaya Aura Communication Manager (CM)
    feature categories 38
Avaya courses 60
Avaya G450 CLI Reference 59
Avaya telephones, which supported 55

B

Branch Gateway 18
    Agent 39
Branch Gateway capacities
    G450 52
Branch Gateway services
    audio related feature 39
    MGC (Media Gateway Controller) 36
    overview 34
    physical media 35
    Voice over IP (VoIP) 51
    voice related features 39
    VoIP (Voice over IP) 34
Buttons
    ASB 16
    RST 16

C

Cable
    required 30
Call center features 39
Calls, preserving 36
CCA port 16
CLI documentation 59
CM, see Avaya Aura Communication Manager 10
Communication Manager
    software uses 38
Components
    optional 20
Console port 16
Contact Closure 39
Continuous telephone services 36

D

Diagnostic tools
    automatic error detection 50
    DP 44
    SNMP 50
Differentiated Services
    SLA 39
Documentation 59
    Avaya G450 CLI Reference 59
    Installing and Upgrading the Avaya Branch Gateway G450 59
    Maintenance Alarms for Avaya Aura Communication Manager, Branch Gateways and Servers 59
    Maintenance Commands for Avaya Aura Communication Manager, Branch Gateways and Servers 59
    Maintenance Procedures for Avaya Aura Communication Manager, Branch Gateways and Servers 59
    Quick Start for Hardware Installation for the Avaya Branch Gateway G430 59
    Quick Start for Hardware Installation for the Avaya Branch Gateway G450 59
document changes 9
DoS attacks 49
Dry contacts 39
Dynamic trap manager 36

E

ECC (External Call Controller) 36
ELS (Enhanced Local Survivability) 36
Embedded Web Manager 49
Emergency Transfer Relay, see ETR 39
Enhanced Local Survivability (ELS) 10
Error Correction Mode 40
ETH LAN port 16
ETH WAN port 16
ETR (Emergency Transfer Relay)
    feature 39
ETR port 16
External Call Controller (ECC) 10

F

Fax over IP 39
Features 13
Fixed LAN port 43
Front panel 16
    LEDs 50

G

G430v3
G430 ... 11
G450 ... 11
Branch Gateway capacties ... 52
G450 1.x ... 16
G450 2.x ... 16
G450 VOIP modules
MP160 ... 30
MP20 ... 30
MP80 ... 30

H

H.248 ... 42
Hardware versions ... 16

I

ICC (Internal Call Controller) ... 36
IEEE 802.1D ... 43
IEEE 802.1w ... 43
InSite Knowledge Base ... 61
Installing and Upgrading the Avaya Branch Gateway G450 59
Internal Call Controller (ICC) ... 10
IP telephones ... 55
IPv6 ... 33

L

LAN
ETH LAN port ... 16
LAN ports
fixed ... 43
switched ... 43
LAN services
overview ... 43
physical media ... 43
port redundancy ... 44
RSTP (Rapid Spanning Tree Protocol) ... 43
VLANs configuration ... 43
LEDs ... 50
legal notice ...
List Measurement ... 41
List Trace ... 41
LLDP (Link Layer Discovery Protocol) ... 44
log file generation ... 42

M

Management
access permissions ... 49
alarms and troubleshooting ... 50
applications ... 48
Management tools ... 48
Management tools *(continued)*
Command Line Interface (CLI) ... 48
Device manager ... 49
Embedded Web Manager ... 49
integrated management ... 49
Manuals ... 59
Avaya G450 CLI Reference ... 59
Installing and Upgrading the Avaya Branch Gateway G450 ... 59
Maintenance Alarms for Avaya Aura Communication Manager, Branch Gateways and Servers ... 59
Maintenance Commands for Avaya Aura Communication Manager, Branch Gateways and Servers ... 59
Maintenance Procedures for Avaya Aura Communication Manager, Branch Gateways and Servers ... 59
Quick Start for Hardware Installation for the Avaya Branch Gateway G450 ... 59
Media Gateway Controllers, see MGC ... 36
Media modules
analog ... 23–25
BRI ... 27, 29
capacity ... 32
DCP ... 26
E1/T1 ... 27
E1/T1 WAN ... 29
MM340 ... 29
MM342 ... 29
MM710 ... 27
MM710B ... 27
MM710B features ... 27
MM710 features ... 27
MM711 ... 23
MM712 ... 26
MM714 ... 24
MM714B ... 25
MM716 ... 25
MM717 ... 26
MM720 ... 27
MM722 ... 29
permitted slots ... 31
slot configuration ... 31
supported ... 20
telephony ... 23
universal serial data WAN ... 29
WAN ... 29
MGC (Media Gateway Controller)
8xxx server management ... 38
backup options ... 10
location ... 10
modes ... 10
overview ... 36
primary ... 10
supported models ... 10
supported servers ... 36
minimum firmware requirements ... 11
MM340 media module ... 29
MM342 media module ... 29

MM710B media modules 27
MM710 media modules 27
MM711
features 24
MM711 media module 23
MM712 media module 26
MM714
features 25
MM714B media module 25
MM714 media module 24
MM714 ports 24
MM716
features 26
MM716 media module 25
MM716 ports 25
MM717 media module 26
MM720 media module 27
MM721
administration modes 28
front panel 29
overview 28
MM722 media module 29
Modem over IP 39, 41, 42
MP160 42
MSS notifications 49

N

new 18

O

Optional components 20

P

packet sniffing 51
Physical description 16
Port mirroring 43
Port redundancy 44
Port registration 42
Ports
CCA 16
Console 16
ETH LAN 16
ETH WAN 16
ETR 16
for telephone lines 35
for telephones 35
LAN 43
SERVICES 16
USB 16
Power cord specifications 58
Primary MGC 10

Q

Quick Start for Hardware Installation for the Avaya Branch Gateway G450 59
Quick Start for Hardware Installation for the Avaya G350 Branch Gateway 59

R

RADIUS server 49
Routing features 47
RST button 16
RSTP (Rapid Spanning Tree Protocol) 43
RTP-MIB 51

S

S8300
capacities 53
S8300D
configuration 21
S8300D Server
components 21
software 21
S8300E Server components 22
S8300E Server configuration 22
S8300E Server hardware requirements 22
S8300E Server software 23
S8300 server
as SRS 10
in standalone deployment 10
supported 10
S8400 server 10
S8500 server 10
S8510 server 10
S8710 server 10
S8720 server 10
S8730 server 10
SCP 49
Security features 49
Services
Branch Gateway 34
LAN 43
summary 33
telephone 34
SERVICES port 16
SLA (Service Level Agreement Monitor) 39
SNMP 49–51
specifications 57
SRS (Survivable Remote Server) 10, 36
SSH 49
Standalone deployment 10
Standard Local Survivability (SLS) 10
STP (Spanning Tree Protocol) 43
support 61
Survivability 10, 36
Switched LAN ports 43

SYN cookies 49

T

T.38 40
Telephones
    outside lines 35
    ports for different types 35
    services 34
    supported 35
    which supported 55
telephones, analog 56
telephones, IP 55
training 60
Transport Layer Security 49
troubleshooting
    packet sniffing 51
Troubleshooting
    automatic error detection 50
    front panel LEDs 50
    LDP 44
    SNMP 50
Troubleshooting and alarms 50
TTY over IP 39

U

USB port 16

V

V.150.1 41
videos 60
VLAN features 43
Voice over IP (VoIP) services 34, 51
VPN 49

W

WAN
    ETH WAN port 16
WAN features 45
    access control lists 45
    inter-gateway alternate routing (IGAR) 45
    policy based routing 45
    RTP header compression 45
    TCP header compression 45
WAN media modules 29
WAN services
    overview 44
    physical media 44
    routing features 47
what's new 18
what's new in 7.1.2 18