Avaya G430 Branch Gateway Overview and Specification

Release 7.0.1
03-603235
Issue 2
July 2016

© 2010-2016, 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. 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 Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

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

multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than 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 that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Product Safety Standards

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

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.

- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

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

For a Class B digital device or peripheral:

Note:

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

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

Equipment With Direct Inward Dialing ("DID"):

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

Proper Answer Supervision is when:

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

Permissible exceptions are:

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

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

Automatic Dialers:

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

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

Toll Restriction and least Cost Routing Equipment:

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

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

For equipment approved prior to July 23, 2001:

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

For equipment approved after July 23, 2001:

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

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

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

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

Means of Connection:

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

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

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

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

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

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

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

Installation and Repairs

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

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

FCC Part 68 Supplier's Declarations of Conformity

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

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

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

Canadian Conformity Information

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

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

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

European Union Declarations of Conformity

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

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

European Union Battery Directive

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

Japan

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

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

If this is a Class A device:

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

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

If this is a Class B device:

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

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, 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

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
2.0	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*.

Note:

This section only talks about what's new in the document structure. To learn what's new in Avaya Aura® Application Enablement Services 7.1, see *Chapter 3: New in this release* later in this guide.

Related resources

Documentation

Title	Description	Number
Installation		
Quick Start for Hardware Installation: Avaya G430 Branch Gateway	An installation guide covering assembly and basic configuration of the *G430*	03-603236
Deploying and Upgrading Avaya G430 Branch Gateway	Describes how to install and upgrade the *G430*, prepare the *G430* for software configuration, and perform some basic configurations. This guide describes how to insert media modules and connect external devices to the *G430* and media module ports.	03-603233
Administration		
Administering Avaya G430 Branch Gateway	Describes how to configure and manage the G430 after it is already installed. This guide contains detailed information about all the features of the G430 and how to implement them.	03-603228
Avaya Branch Gateway G430 CLI Reference	Describes the commands in the G430 CLI.	03-603234
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
Implementation		
Operations Intelligence Suite Advanced Implementation Guide for SLA Mon	Describes installation and Configuration of Service Level Agreement Monitor	100167328

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. 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.

Warranty

Avaya provides a 90-day limited warranty on Branch Gateway. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Branch Gateway in the warranty period is available on the Avaya Support website at https://support.avaya.com under **Help & Policies> Policies & Legal > Warranty & Product Lifecycle**. See also **Help & Policies > Policies & Legal > License Terms**.

Chapter 2: G430 Branch Gateway overview

G430 Branch Gateway Overview

Avaya Branch Gateway G430

The Branch Gateway G430 is a multipurpose gateway targeting small and medium branches of 1 to 150 users. The G430 supports two expansion modules to support varying branch office sizes.

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 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

G430 is a scalable device with a basic configuration consisting of one power supply unit (PSU) and 256 MB RAM. G430 v1 has one on-board VoIP module providing 25 VoIP channels for G.711 and G.726 and 20 channels for G.729, and an additional slot for the optional insertion of an MP10, MP20, MP80, or MP120 VoIP module. If an MP120 is installed on G430 v1, the on-board VOIP module is disabled. G430 v2 has no on-board VOIP module. You can also replace the 256 MB RAM with 512 MB RAM and use an external compact flash to increase the number of announcement files from 256 to 1024 and increase announcement time from 45 minutes to 4 hours.

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, Ethernet WAN lines, and external routers, three slots are provided for plugging in optional media modules. Two EM200 expansion modules can be connected to the G430, providing two media module slots each, bringing the total number of available media module slots to seven. Pluggable media modules provide interfaces for different types of telephones and trunks. 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 G430 features field replaceable RAM memory card and DSP childboard.

Minimum firmware requirements for G430

Firmware version	Build	v1a	v2a (MP120 Preinstalled)	Comments	Recommended CM Version - Older versions of CM will work
BGW 5.2.1	30.28.0	Yes	No	No BGW support MP120	CM 5.2.1(SP 16) or higher (CM blocks more than 105 channels)
BGW 6.1	31.26.0	Yes	No	No BGW support MP120	CM 6.0.1 (CM blocks more than 105 channels)
BGW 6.2.1	32.26.0	Yes	No	No BGW support MP120	AA 6.2 FP1 CM 6.2 sp 4 — Dec 2012 (CM blocks more than 105 channels)
BGW 6.3	33.13.0	Yes	No	No BGW support MP120	AA 6.2 FP2 CM 6.3 — May 2013 (CM supports all 120 channels)
BGW 6.3.1	34.6.0	Yes	No	No BGW support MP120	AA6.2 FP3 CM6.3.2 — Oct 2013 (CM supports all 120 channels)

Table continues…

Firmware version	**Build**	**v1a**	**v2a** **(MP120 Preinstalled)**	**Comments**	**Recommended CM Version** **- Older versions of CM will work**
BGW 6.3.5	35.x.y	Yes	Yes	MP120 Support V150.1 Features	AA 6.2 FP3 CM 6.3.2 + (CM supports all 120 channels)
BGW 6.3.6 JITC	36.x.y	Yes	Yes	MP120 Support	AA 6.2 FP 4 CM 6.3.6 AA 6.2 FP3 CM 6.3.2 + (CM supports all 120 channels)
BGW 6.3.7	36.16.0 +	Yes	Yes	MP120 Support	AA 6.2 FP 4 CM 6.3.6 +
BGW 6.3.8	36.16.0 +	Yes	Yes	MP120 Support	AA 6.2 FP 4 CM 6.3.6 +
BGW 6.3.9	36.16.0 +	Yes	Yes	MP120 Support	AA 6.2 FP 4 CM 6.3.6 +
BGW 6.3.10	36.16.0 +	Yes	Yes	MP120 Support	AA 6.2 FP 4 CM 6.3.6 +
BGW 6.3.11	36.16.0 +	Yes	Yes	MP120 Support	AA 6.2 FP 4 CM 6.3.6 +
BGW 6.3.12	36.16.0	Yes	Yes	MP120 Support	AA 6.2 FP 4 CM 6.3.6 +
BGW 6.3.13	36.17.0	Yes	Yes	MP120 Support	AA 6.2 FP 4 CM 6.3.6 +
BGW 7.0	37.20.0	Yes	Yes	MP120 Support	AA 7.0, CM 7.0 AA 6.2 FP 4 CM 6.3.6 +
BGW 7.0.0.1	37.20.0	Yes	Yes	MP120 Support	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	MP120 Support	AA 7.0, CM 7.0 AA 6.2 FP 4 CM 6.3.6 +
BGW 7.0.1	37.38.0	Yes	Yes	MP120 Support	AA 7.0 FP 1, CM 7.0.1 AA 7.0, CM 7.0 + AA 6.2 FP 4, CM 6.3.6 +

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	• 3-slot chassis (three slots for media modules) • Two EM200 expansion modules, each providing two slots each for media modules • Hot-swappable media modules • Support for hot-swappable external compact flash • VoIP DSPs (up to 105 channels) • Memory SoDIMMs
Voice features	• H.248 gateway • Voice line interfaces: - IP phones - Analog phones - Avaya DCP phones - BRI Phones - FXS/Fax - VoIP - Fax and modem over IP • Voice trunk interfaces: - FXO - 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 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

Table continues…

Feature type	Description
Routing and WAN features	✱ **Note:** IPv6 is not supported on the WAN. • One WAN 10/100 Ethernet port with traffic shaping capabilities • PPPoE (IPv4 only) and PPP (IPv4 only) • Routing Protocols: Static, OSPF, RIP • VRRP (IPv4 only) • Equal Cost Multi Path routing (ECMP) • IPSec VPN • cRTP • WAN Quality of Service (QoS) • Policy-based routing • DHCP relay • GRE tunneling • Dynamic IP addressing (DHCP client/PPPoE) • Object tracking • Backup Interface
LAN features	• Two LAN 10/100 RJ-45 Ethernet ports (w/o POE) • Auto-negotiation • 2K MAC table with aging • 8 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

Table continues…

Feature type	Description
	• Access list support
Management features	• Avaya Device Manager • Embedded Web Manager (IPv4 only) • RADIUS Authentication support (IPv4 only) • SNMPv1 traps and SNMPv3 notifications • SNMPv1 and SNMPv3 servers support • 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

G430 physical description

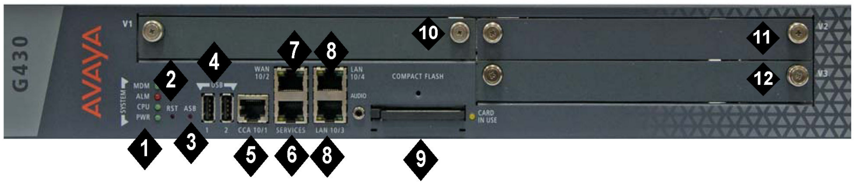


Figure 1: The Branch Gateway G430 Chassis

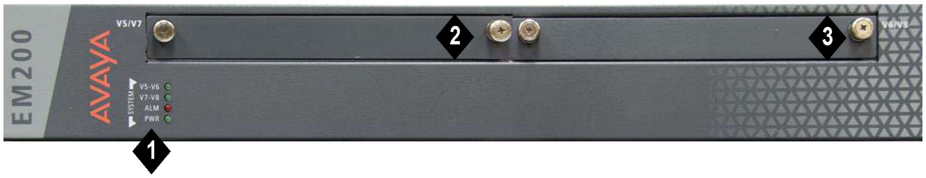
No	Name	Description
1	System LEDs	LEDs that indicate the status of the system
2	RST button	Reset button. Resets chassis configuration.
3	ASB button	Alternate Software Bank button. Reboots the G430 with the software image in the alternate bank.
4	USB ports	Two USB 2.0 ports with USB connectors. Supports the connection of: • USB flash drive. No more than one USB flash drive can be connected. • USB modem: Multitech MultiModemUSB MT5634ZBA-USB-V92, or USRobotics USB

Table continues…

No	Name	Description
		modem model 5637. No more than one USB modem can be connected.
5	CCA (Contact Closure) port	RJ-45 port for ACS (308) contact closure adjunct box.
6	Services	Ethernet 10/100 port for services and maintenance access. RJ-45 connector.
7	WAN 10/2	One 10/100 Base TX Ethernet WAN port. RJ-45 connector.
8	LAN 10/4	Two 10/100 Base TX Ethernet LAN ports. RJ-45 connectors.
9	Compact Flash	Compact Flash slot
10	V1	Slot for media module or S8300 Server
11	V2	Slot for media module
12	V3	Slot for media module

For information about the different media modules that can be housed in the G430 media module slots, see Chapter 2: Optional components on page 21.

EM200 physical description



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

For information about the different media modules that can be housed in the EM200 media module slots, see Chapter 2: Optional components on page 21.

Chapter 3: New in this release

What's new in Branch Gateway

This chapter provides an overview of the new features and enhancements for Branch Gateway 7.1.

CLI Commands

Two new CLI Commands are introduced in Release 7.1:

- **`set allow-unencrypted`**: System administrator can use this command to allow or disallow media encryption requests from Communication Manager.
- **`set link-encryption`**: System administrator can use this command to specify what TLS versions will be offered by the gateway when connecting to a server.

FIPS-mode

FIPS-mode is a feature that is currently not supported in Release 7.1 for use by our customers since it is pending FIPS certification by a 3rd-party at this time. It is targeted to be available in a post 7.0.1 release after achieving FIPS certification.

OPUS Codec

The MP120 and MP160 VOIP modules are now capable of supporting the Opus codec in narrowband mode.

Chapter 4: Optional components

Optional components

The Branch Gateway is a versatile device with powerful capabilities that can be expanded to include up to two EM200 expansion modules. To implement the various services that are supported, a variety of swappable internal components called media modules are available.

Supported media modules

Media module	Description	Comment
S8300 C/D/E	Communication Manager server	In slot V1 only
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	

⚠ **Caution:**

The MM340 and MM342 are not supported by the Avaya Branch Gateway G430. Do not insert an MM340 or MM342 media module into an G430 Branch Gateway.

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
- One internal Compact Flash drive, which is used as the primary reboot device
- Modem support for alarming

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
    - Enabling and disabling the modem
    - 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 5.2 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
- Ethernet LAN port reserved for future use
- USB port for DVD Drive
- Two DIMM sockets
- USB compact flash reader
- 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
  - Enabling and disabling the modem
  - 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

Utility Services overview

From Utility Services Release 7.0, you can deploy Utility Services as a standalone OVA.

Out of Band Management

Out of Band Management is a physically and logically separate network connection. It connects to a customer's private IT management network and provides for secure management and administration of Avaya products.

From Utility Services Release 7.0.1, you can activate out-of-band management even after deployment.

Utility Services Release 7.0.1 and later support a full out of band management configuration. Therefore, you can deploy Utility Services with two IP addresses and split the user and management traffic to different Ethernet interfaces on different IP networks.

When Utility Services is set for out of band management, the following services are allocated for full or Utility Services-only mode:

Application	Interfaces for traffic
Phone firmware download	Public
Phone settings file	Public
Gateway firmware download	Public
DHCP Server	Public
Myphone User	Public
SSH	Out of Band Management / Services
Myphone Admin	Out of Band Management
CDR connection to CM	Out of Band Management
Main admin web pages	Out of Band Management / Services
Alarm source	Out of Band Management
SAL connection (SSH, HTTP)	Out of Band Management

When Utility Services is set for out of band management, the following services are allocated for services port-only mode:

Application	Interfaces for traffic
SSH	Out of Band Management / Services
Alarm source	Out of Band Management
SAL connection (SSH, HTTP)	Out of Band Management
Main admin web pages	Disabled
Phone firmware download	Disabled
Gateway firmware download	Disabled
Phone settings	Disabled
Gateway firmware download	Disabled
DHCP Server	Disabled
Myphone Server	Disabled
CDR connection to CM	Disabled
Myphone admin	Disabled

Note:

If a network is not mentioned for service when Out of Band Management is enabled, the service must be disabled on that interface.

Utility Admin

With Utility Services 7.0.1, the Utility Services Administration Web Pages are accessible on port 543.

The URL is https:// <Utility Services IP> :543/admin.html.

‘Utility Services IP’ is the Public IP address of Utility Services when OOBM is disabled. This is the OOBM IP address of Utility Services when OOBM is enabled.

With the Utility Admin page, you can configure and gain access to the following elements:

- Software Version: Displays the software versions of packages, operating system, IP telephone firmware, media module firmware, and gateway firmware that are active on Utility Services.
- Firewall Rules: Displays the IPv4 and IPv6 firewall rules of Utility Services.
- IP Phone file server: Supports the download of the IP telephone firmware and the settings files. The server also supports backing up and restoring of IP telephone user configuration, for example, speed dial configurations.
- ADVD Settings Editor: Provides a Web-based tool for configuring the Avaya Desktop Video Device (ADVD) settings file. ADVD Settings Editor provides enhanced validation to avoid wrong configurations.
- IP Phone Settings Editor: Provides a Web-based tool for configuring the IP telephone settings file. IP Phone Settings Editor provides enhanced validation to avoid wrong configurations.
- IP Phone firmware management: Supports the upload of the new telephone firmware to the file server.
- DHCP server: Provides basic DHCP server capabilities for supporting IP telephones.
- IPv6 DHCP server: Provides IPv6 DHCP server capabilities for supporting IP telephones.
- IP Phone Push Server: Displays the content from Push Server Database.
- Log viewer: Provides access of the log files for the Utility Services applications.
- CDR tools: Provides a Call Detail Record (CDR) collection capability. The CDR tool collects the CDR records from Communication Manager and imports the records into the Utility Services database. The CDR tool also provides simple examples on using the CDR data in the database.

MyPhone Admin

With Utility Services 7.0.1, the Utility Services MyPhone Administration Web Pages are accessible on port 9443.

The URL is `https://<Utility Services IP>:9443/MyPhoneAdmin`.

‘Utility Services IP’ is the Public IP address of Utility Services when OOBM is disabled. This is the OOBM IP address of Utility Services when OOBM is enabled.

With the MyPhone Admin page, you can gain access to the following configuration elements of MyPhone and IP telephone operations:

- MyPhone Feature Buttons: Enable or disables the features available to the MyPhone users.
- WML Links: Displays the default Wireless Markup Language (WML) page on the IP telephones. You can use this element to configure the default WML page.
- System Message: Configures the WML page. This element contains a block of text that is relevant to every IP telephone user.

For more information about MyPhone Admin, see *Accessing and Managing Avaya Aura® Utility Services*, 03-603628.

MyPhone

With the MyPhone page, you can:

- Configure the IP telephones.
- Configure buttons, language settings, EC500, Enhanced Call forwarding, and other features.
- Configure the security codes and other parameters.

For more information about MyPhone, see *Accessing and Managing Avaya Aura® Utility Services*, 03-603628.

MyPhone User Guide

You can download a PDF file or an online HTML file to view the MyPhone documentation.

Deploying Utility Services

You can deploy Utility Services on the following:

- VMware

  For more information, see *Deploying Avaya Aura® Utility Services* guide.
- Appliance Virtualization Platform through Solution Deployment Manager (SDM)

  For more information, see *Deploying Avaya Aura® applications from System Manager*.

Audit Account Addition

Utility Services supports an auditor account. You can use the auditor account to view the configuration and log files on Utility Services. However, you cannot alter any configuration. During the time of installation, the default password for the auditor account is `audit01`. You can change the default password at any given instance by starting an SSH session to Utility Services.

IP Phone Firmware Removal

Utility Services no longer bundles the IP Phone firmware within the build. To ensure that Utility Services has the correct IP Phone firmware for the installation, you must download the latest version of the firmware from PLDS. You can download the latest IP Phone firmware to store on Utility Services at any time. The IP Phone firmware management features remain unchanged from the previous versions.

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

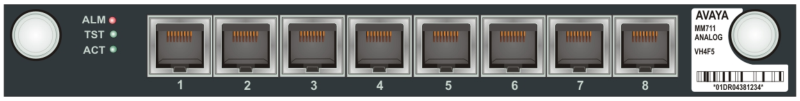


Figure 2: The MM711 media module

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

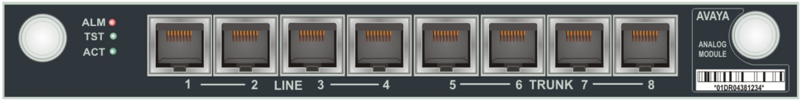


Figure 3: The MM714 media module

MM714B analog media module

The MM714B analog media module provides all the features provided by the MM714 (see MM714 analog media module on page 28), 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.

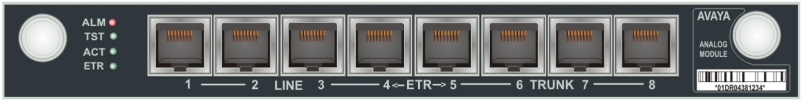


Figure 4: The MM714B media module

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.

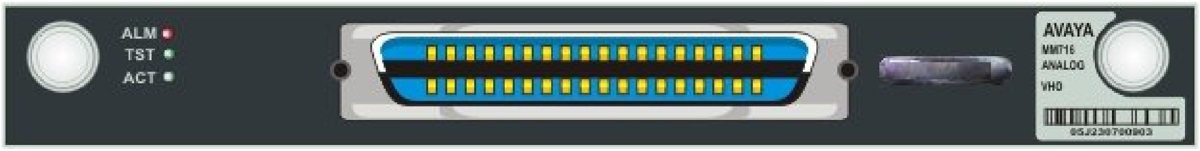


Figure 5: The MM716 media module

VOIP Modules in G430

A media processor or a VOIP module provides the resources/channels to support voice, modem, fax calls over IP.

G430 supports the VOIP modules listed in the table below:

VOIP Modules	Description

Table continues…

MP10	Supports a maximum of 10 channels.
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
MP120	Supports a maximum of 120 channels. The MP120 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 media processors. G430 supports a maximum of 120 channels. If an MP120 is installed on a G430 v1, the onboard VoIP module will be disabled. Supports a maximum of 60 channels with the Opus codec.

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 48 for a list of compatible DCP telephones.

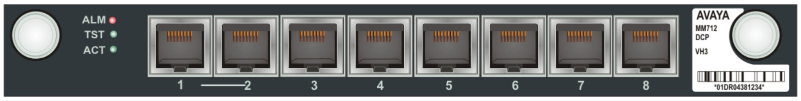


Figure 6: The MM712 media module

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.

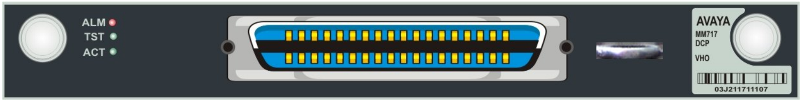


Figure 7: The MM717 media module

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

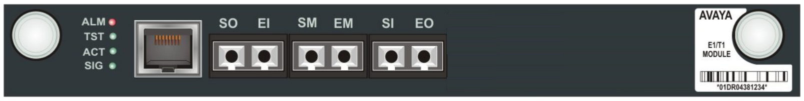


Figure 8: The MM710B media module

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.

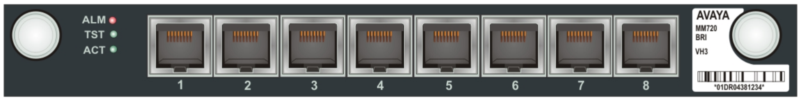


Figure 9: The MM720 media module

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.

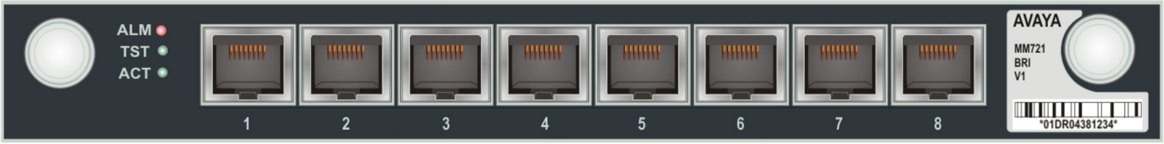
Note:

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 32.

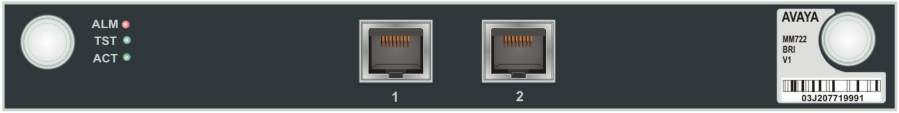


Figure 10: The MM722 media module

Note:

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

Media module slot configurations

When choosing a combination of media modules to install in the Branch Gateway chassis and EM200 expansion modules, 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 G430 chassis has three media module slots, marked V1, V2, and V3. Each of the two optional EM200 expansion modules has two media module slots each. SeeEM200 physical description on page 19. The slots of the EM200 connected to the EXPANSION OUT 1 connector on the rear of the G430 are slots V5 and V6, and the slots of the EM200 connected to the EXPANSION OUT 2 connector on the rear of the G430 are slots V7 and V8.

Table 1: Permitted slots for media modules

Media module	Permitted slots
MM710, MM710B	Any media module slot: V1-V3, V5-V8.
MM711	Any media module slot: V1-V3, V5-V8
MM712	Any media module slot: V1-V3, V5-V8
MM714, MM714B	Any media module slot: V1-V3, V5-V8
MM716	Any media module slot: V1-V3, V5-V8
MM717	Any media module slot: V1-V3, V5-V8
MM720	Any media module slot: V1-V3, V5-V8
MM721	Any media module slot: V1-V3, V5-V8
MM722	Any media module slot: V1-V3, V5-V8
S8300 C/D	V1

G430 and EM200 media module capacity

The G430 chassis is designed to accommodate:

- Up to three of the following telephony media modules: MM710, MM710B, MM711, MM712, MM714, MM714B, MM720, MM721, MM722
- Up to two of the following telephony modules: MM716, MM717
- Up to one S8300 server (in slot V1 only)

Each EM200 chassis is designed to accommodate:

- Up to two of the following telephony media modules: MM710, MM711, MM712, MM714, MM714B, MM716, MM717, MM720, MM721, MM722

Note:

Although you can insert a total of seven MM710 media modules in the extended G430 (a G430 with two EM200 expansion modules), the optimum number is four MM710 media modules, since the G430 can support up to 120 VoIP channels.

Note:

Although you can insert a total of seven MM721 media modules in the extended G430 (a G430 with two EM200 expansion modules), the maximum number allowed is four MM721 media modules.

Chapter 5: Summary of services

Summary of services

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 support up to eight 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

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:

- PPPoE (ADSL modem)
- Ethernet-DHCP/static IP (cable modem)

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.
- The Branch Gateway has the ability to map several PPP sessions to a single E1/T1 interface.
- PPPoE
- Backup functionality supported between any type of Layer 2 interface except for the VLAN interface
- Dynamic Call Admission Control (CAC) for Fast Ethernet 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 Application

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 Services port.
- Telnet through the network
- Telnet through dialup, using a dialup PPP network connection

  Note:

  Telnet is disabled by default on the Branch Gateway
- 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 G430 CLI Reference*.

For information about how to use the CLI to perform specific configuration tasks, see *Administration for the Avaya Branch Gateway G430*.

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 in one of the following ways:

- From Avaya Integrated Management software
- From a web browser on a computer on the same network as the device

For information about Avaya Branch Gateway Manager, see the *Avaya Integrated Management Manager User Guide*.

Avaya Integrated Management

Avaya Integrated Management offers a comprehensive set of web-based network and system management solutions that support Avaya converged voice solutions. You can use Avaya Integrated Management to monitor SNMP traps on the Branch Gateway. You can also use Avaya Integrated Management to access Avaya Gxxx Manager.

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
- ASG authentication for remote service logins. ASG 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 G430* 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

Maximum Branch Gateway G430 capacities

Table 2: Branch Gateway G430 capacities

Description	Capacity	Comments
Maximum number of G430s controlled by an External Call Controller (ECC).	250	This number also applies if the same external server controls a combination of Avaya Branch Gateways G430, G450, G350, G250, and G700.
Maximum number of G430s controlled by an ECC server housed in another Branch Gateway G430 (or G450 or G700).	50	This number also applies if the same external server controls a combination of Avaya Branch Gateways G430, G450, G350, G250, and G700.
Maximum total number of telephones supported by the G430.	150	This number can be higher when connected to Communication Manager, depending on configuration. When connected to SLS, a maximum of 150 IP stations may be registered.
Maximum number of IP telephones per Branch Gateway G430.	150	
Maximum number of analog phones per Branch Gateway G430.	56 104 for a G430 with one EM200 152 for a G430 with two EM200s	
Maximum number of DCP phones per Branch Gateway G430.	56 104 for a G430 with one EM200 152 for a G430 with two EM200s	

Table continues…

Description	Capacity	Comments
Maximum number of BRI endpoints per Branch Gateway G430.	48 80 for a G430 with one EM200 112 for a G430 with two EM200s	Maximum of 64 when the BRI modules are MM721.
Simultaneous two-way conversations with TDM transcoding from IP phone to legacy telephone or trunk.	120	
Simultaneous two-way conversations with TDM transcoding from TDM phones to IP phones	120	
Maximum number of BRI trunks	24 40 for a G430 with one EM200 56 for a G430 with two EM200s	Maximum of 32 when the BRI modules are MM721
Maximum number of PSTN trunks	4 T1 3 E1	7 E1/T1 can be supported in tandem mode
Miscellaneous		
Simultaneous fax transmissions	120	Fax transmissions using VoIP resources
Touch-tone recognition (TTR)	32	
Tone Generation	unlimited	
Announcements ports	15 ports for playback 1 for record	

S8300 maximum capacities

Table 3: 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

Table continues…

Item	Quantity Supported
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*.

H.323 stations using TLS

H.323 stations using TLS are supported since Avaya Aura 6.2 FP4 with up to 2,000 endpoints per Communication Manager (CM). This feature was, however, limited to USA Department of Defense (DOD) customers.

Beginning with Avaya Aura® Release 7.0.1, support for H.323 stations using TLS is now generally available (GA) for all customers. The capacity is now increased up to 18,000 endpoints per CM. For a Branch Gateway with S8300 the capacity is limited up to 1,000 H.323 TLS endpoints.

See *Avaya Aura ® Communication Manager System Capacities Table* for detailed information regarding capacities.

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 G430 supports all Avaya IP telephones, including the Avaya 1602, 1608, 1616 H.323 and 96xx IP phones, except for the Avaya 4630 IP Screenphone.

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 8410 and 8410D Digital Telephones
- Avaya 8434DX Digital Telephone
- IP softphones that are configured as “Road Warrior” and “Take Over” a DCP station

- Definity Extender – ISDN single endpoint 302 series Attendant Console (302D)
- Avaya 603E Call Master III
- Avaya 606B1 Call Master VI
- 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
- Avaya 2500 analog Telephone

Chapter 9: Technical specifications

Technical specifications

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

Specifications

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

Table 4: Avaya Branch Gateway G430 specifications

Description	Value
Height	2.62 in. (66.5 mm)
Width	19 in. (482.6 mm)
Depth	12.8 in. (325 mm)
Weight of empty chassis	under 11 pounds (under 5 Kg)
Weight of chassis with basic configuration	between 13 and 14 pounds (between 6 and 7 Kg)
Ambient working temperature	32° to 104°F (0° to 40°C)
Storage temperature	–40°F to 150°F (–40°C to 66°C)
Operation altitude	up to 10,000 ft. (3000 m)
Front clearance	12 in. (30 cm)
Rear clearance	18 in. (45 cm)
Humidity	10-90% relative humidity, non-condensing
Voltage	90V to 264V AC, 48 to 63 Hz
Power rating	800 BTU/h (234 W)
Max current	2.4 A

EM200 specifications

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

Table 5: EM200 specifications

Description	Value
Height	2.62 in. (66.5 mm)
Width	19 in. (482.6 mm)
Depth	12.8 in. (325 mm)
Weight of empty chassis	under 11 pounds (under 5 Kg)
Weight of chassis with media modules and brackets	13 pounds (6 kg)
Ambient working temperature	32° to 104°F (0° to 40°C)
Operation altitude	up to 10,000 ft. (3000 m)
Front Clearance	12 in. (30 cm)
Rear Clearance	18 in. (45 cm)
Humidity	10 to 90% relative humidity, non-condensing
Power rating	90V to 264V AC, 48 to 63 Hz
BTU	430 BTU/h
Max current	1.3 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 6: 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)

Index