Overview for the Avaya G450 Branch Gateway

6.1
03-602058
Issue 4
November 2010

Notice

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

Warranty

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

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

Disclaimer

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

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Product Safety Standards

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

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

This product may contain Class 1 laser devices.

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

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

For a Class B digital device or peripheral:

Note:

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

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

Equipment With Direct Inward Dialing ("DID"):

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

Proper Answer Supervision is when:

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

Permissible exceptions are:

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

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

Automatic Dialers:

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

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

Toll Restriction and least Cost Routing Equipment:

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

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

For equipment approved prior to July 23, 2001:

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

For equipment approved after July 23, 2001:

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

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

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

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

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

Means of Connection:

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

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

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

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

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

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

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

Installation and Repairs

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

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

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a 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

CE

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

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

European Union Battery Directive

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

Japan

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

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

If this is a Class A device:

This is a Class 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。

Downloading Documentation

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

Contents

Chapter 1: About this book

About this book

This guide contains information that you need to consider before implementing the Avaya G450 Branch Gateway. Use this guide to learn what the G450 can do and to plan how you will deploy a G450 in your environment.

Audience

The information in this book is intended for use by Avaya technicians, provisioning specialists, Business Partners, and customers.

Related documents

Title	Description	Number
Quick Start for Hardware Installation for the Avaya G450 Branch Gateway	A concise installation guide covering assembly and basic configuration of the *G450*	03-602053
Installing and Upgrading the Avaya G450 Branch Gateway	Describes how to install and upgrade the *G450*, prepare the *G450* for software configuration, and perform some basic configurations. This guide describes how to insert media modules and connect external devices to the *G450*	03-602054

Title	Description	Number
	and media module ports.	
Administration for the Avaya G450 Branch Gateway	Describes how to configure and manage the G450 after it is already installed. This guide contains detailed information about all the features of the G450 and how to implement them.	03-602055
Avaya G450 Branch Gateway CLI Reference	Describes the commands in the G450 CLI.	03-602056
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

Chapter 2: Introduction to Branch Gateways

Introduction to Branch Gateways

Avaya G450 Branch Gateway

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

The G450 Branch Gateway can support up to 450 users when deployed as a Branch Gateway in a mid to large branch office of a large enterprise or a call center. This requires Avaya Aura®Communication Manager IP telephony software running on one or more Avaya S8XXX Servers. The Avaya S8300 Servers supports 50 Branch Gateways, the other Avaya Media Servers support up to 250 Branch Gateways.

Related topics:

Branch Gateway functions on page 11

Branch Gateway functions

The Branch Gateway:

- Works in conjunction with Avaya Aura® Communication Manager IP telephony software running on Avaya S8XXX Servers to help deliver intelligent communications to enterprises of all sizes
- Combines telephone exchange and data networking, by providing PSTN toll bypass, and routing data and VoIP traffic over the WAN
- Features a VoIP engine, an optional WAN router, and Ethernet LAN connectivity.
- Provides full support for Avaya IP and digital telephones, as well as analog devices such as modems, fax machines, and telephones.

Telephone services on an Branch Gateway are controlled by an Avaya S8XXX 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
- The Avaya S88XX and S85XX Servers as ECCs

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

Branch Gateway specifications

The G450 is a scalable device with a basic configuration consisting of one power supply unit (PSU) and 256 MB RAM, and a single DSP childboard supporting either 20 or 80 VoIP channels. This configuration can be enhanced by adding a redundant PSU, up to two RAM modules of 1 GB each, and up to three additional DSP childboards, increasing the number of VoIP channels to 320 channels. You can also add an external compact flash, increasing the number of announcement files to 1024.

The Branch Gateway is a modular device, adaptable to support different combinations of endpoint devices. While fixed front panel ports support the connection of external LAN switches, network data ports, Ethernet WAN lines, and external routers, eight slots are provided for plugging in optional media modules. Pluggable media modules provide interfaces for different types of telephones, trunks, and WAN links. A combination is selected to suit the needs of the branch. A range of telephony modules provides full support for legacy equipment such as analog and digital telephones. A range of WAN modules provide support for Universal Serial Port and E1/T1 WAN links. IP phones are supported via an external LAN switch.

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

Branch Gateway features

Note:
Certain features are supported in IPv4 only.

- Hardware features:
  - 9-slot chassis (one slot for main board and eight slots for media modules)
  - Swappable main board module

- Hot-swappable media modules
- Support for hot-swappable external compact flash
- Support for two load sharing hot-swappable power supply units
- Hot-swappable fan tray
- VoIP DSPs (up to 240 channels)
- Memory SIMMs

• 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
- Survivability features for continuous voice services:
    - Local Survivable Processor (LSP) (with S8300)
    - Standard Local Survivability (SLS) (IPv4 only)
    - Emergency Transfer Relay (ETR)
    - Modem Dial Backup
    - Dynamic Call Admission Control (CAC) for Fast Ethernet, Serial, and GRE tunnel interfaces
    - Inter-Gateway Alternate Routing (IGAR)
- DHCP and TFTP server to support IP phones images and configuration (IPv4 only)
- Announcements and Music on Hold (MoH) support
- Contact Closure support

• Routing and WAN features:

Note:

IPv6 is not supported on the WAN.

- Two WAN 10/100 Ethernet ports with traffic shaping capabilities
- T1/E1 and USP interfaces
- PPPoE (IPv4 only), Frame-relay, and PPP (IPv4 only)
- Routing Protocols: Static, OSPF, RIP
- VRRP (IPv4 only)
- Equal Cost Multi Path routing (ECMP)
- IPSec VPN
- cRTP
- WAN Quality of Service (QoS)
- Policy-based routing
- DHCP relay
- GRE tunneling
- Dynamic IP addressing (DHCP client/PPPoE)
- Object tracking
- Backup Interface

• LAN features:

- Two LAN 10/100/1000 RJ-45 Ethernet ports (w/o POE)
- Auto-negotiation
- 4K MAC table with aging
- 64 VLANs
- Multi-VLAN binding, 802.1Q support
- Ingress VLAN Security
- Broadcast/Multicast storm control
- Automatic MAC address aging
- Rapid Spanning Tree
- Port mirroring
- RMON statistics
- Port redundancy
- LLDP (IPv4 only)

• Security hardened gateway features:

- Media and signaling encryption

- Secured management
- Digitally signed gateway firmware
- Managed security service support
- Access list support

• Management features:

- Avaya Device Manager
- Embedded Web Manager (IPv4 only)
- RADIUS Authentication support (IPv4 only)
- SNMPv1 traps and SNMPv3 notifications
- Telnet (IPv4 only) and SSHv2 support
- SCP, TFTP, and FTP clients
- Syslog client
- Modem access for remote administration
- Packet Sniffing
- RTP-MIB
- Backup and Restore on USB Flash drive

G450 physical description

There are two hardware versions of the G450, referred to as *G450 1.x* and *G450 2.x*. 1.x and 2.x refer to the hardware suffix of the G450, which is printed on the label displayed on the rear of the chassis. The differences between the two versions are minor, and include slightly different front panels, and different placement of components on the main boards.

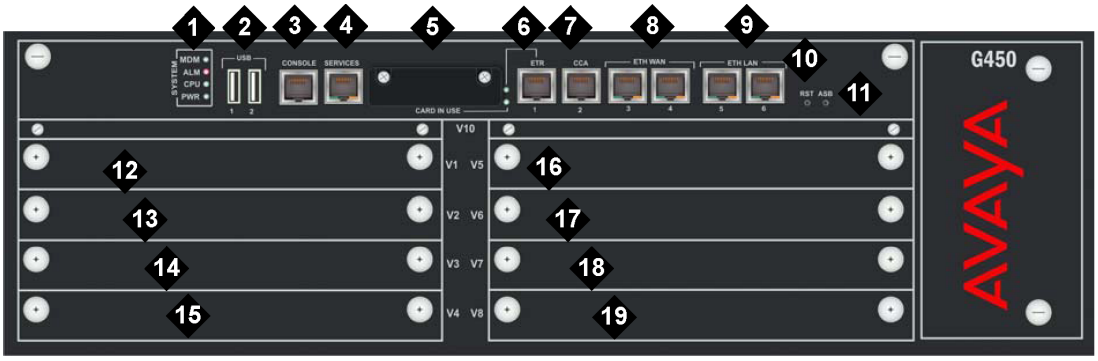


Figure 1: The G450 1.x Branch Gateway Chassis

Figure Notes:

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

For information about the different media modules that can be housed in the G450 media module slots, see Optional components on page 19.

Name	Description
CCA	RJ-45 port for ACS (308) contact closure adjunct box.
ETH WAN	Two 10/100 Base TX Ethernet WAN ports. RJ-45 connectors.
ETH LAN	Two 10/100/1000 Base TX Ethernet LAN ports. RJ-45 connectors.
CONSOLE	RS-232 port for services and maintenance access. RJ-45 connector.
SERVICES	Ethernet 10/100 port for services and maintenance access. RJ-45 connector.
ETR	Emergency Transfer Relay port. Controls two external 808A emergency transfer panels. RJ-45 connector.
USB	Two USB 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 modem model 5637. No more than one USB modem can be connected.
RST	Reset button. Resets chassis configuration.

Name	Description
ASB	Alternate Software Bank button. Reboots the G450 with the software image in the alternate bank.

Chapter 3: Optional components

Optional components

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

Related topics:

Supported media modules on page 19
S8300D hardware requirements on page 20
S8300D Server components on page 20
S8300D Server configuration on page 20
S8300D Server software on page 21
Telephony media modules on page 24
WAN media modules on page 29
Media module slot configurations on page 30

Supported media modules

Table 1: Supported media modules

Media module	Description
S8300	Communication Manager server
Telephony media modules	
MM711	8 universal analog ports
MM714	4 analog telephone ports and 4 analog trunk ports
MM714B	4 analog telephone ports, 4 analog trunk ports, and an emergency transfer relay
MM716	24 analog ports
MM712	8 DCP telephone ports
MM717	24 DCP telephone ports

Media module	Description
MM710 MM710B	1 T1/E1 ISDN PRI trunk port
MM720	8 ISDN BRI trunk or endpoint (telephone or data) ports
MM722	2 ISDN BRI trunk ports
WAN media modules	
MM340	1 E1/T1 data WAN port
MM342	1 universal serial data WAN port

S8300D Media Server

S8300D hardware requirements

The hardware for the S8300D Server as primary controller is identical to the hardware for the S8300D Server as Survivable Remote Server. The difference between the two configurations is entirely in software.

S8300D Server components

For a list of S8300D components used in each S8300D configuration, see Configurations.

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:

- 80-GB hard disk
- 4-GB DRAM (with one 1 GB DIMM)
- 8-GB Internal Solid State Drive (SSD)

- Three 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.
  - Another USB port can be used for a USB modem.
  - A third USB port can be used for a Compact Flash drive.
- One services port
- One internal Compact Flash drive which is used as the primary reboot device
- Modem support for alarming

S8300D Server software

In addition to Communication Manager software for applications, the S8300D Server runs the following software:

- A Web server that is used for:
  - Backing up and restoring customer data
  - Viewing current alarms
  - Server maintenance, including busy out, shutdown, and status of an S8300D Server
  - Security commands to enable and disable the modem
  - Security commands to start and stop the FTP server
  - Security commands to view the software license
  - SNMP access to configure trap destinations and to stop and start the master agent
  - Configuration information about the S8300D Server
  - Upgrading access to the S8300D Server
- Maintenance software
- Linux operating system
- Trivial File Transfer Protocol (TFTP) server
- Secure HTTP server for IP phone file downloads
- H.248 Branch Gateway Signaling Protocol
- Control messages tunneled over H.323 Signaling Protocol

Utility Services overview

The Midsize Business Template Utility Services runs a number of utility applications that support or enhance the Midsize Business Template component applications (Communication Manager, Communication Manager Messaging, SIP Enablement Services, and Application Enablement Services) facilitating a complete single box solution.

These Utility Services applications are briefly discussed in the following sections.

Utility Admin

Utility Admin enables you to configure and access various Utility Services applications, as follows:

- IP Phone file server: Supports the download of IP phone firmware and settings files. It also supports the back up and restore of IP Phone user configuration (for example, speed dial configurations.)
- IP Phone Settings Editor: Provides a web based tool for configuring the IP phone settings file. This significantly simplifies the process of making changes to the IP phone settings file and provides enhanced validation to help avoid mis-configurations.
- IP Phone firmware management: Enables you to upload new phone firmware to the file server.
- DHCP server: Provides basic DHCP server capabilities for supporting IP phones.
- Log viewer: Enables you to access the log files for all of the utility server applications.
- CDR Tools: Provides a CDR (Call Detail Records) collection capability that collects CDR records from Communication Manager and imports them into the Utility Services's database. It also provides some simple example reports to demonstrate how the CDR data in the database could be used by a system administrator.

MyPhone Admin

MyPhone Admin enables you to access some configuration elements of MyPhone and IP Phone operations, as follows:

- MyPhone Feature Buttons: Allows you to enable and disable the features available to the users of MyPhone.
- WML Links: The IP Phones have an ability to display a default WML page. This option enables you to configure the default WML page. On a general MBT installation, the default page provides links to the Avaya Thin-Client LDAP Directory without a web address entry, and a System Message page.
- System Message: Enables you to configure the WML page. This typically contains a block of text which is relevant to every IP Phone user.
- Configure Directory Application: Enables you to configure the Avaya Thin-Client LDAP Directory through four options, namely General Administration, Search Administration, Details Administration, and Softkey Administration.

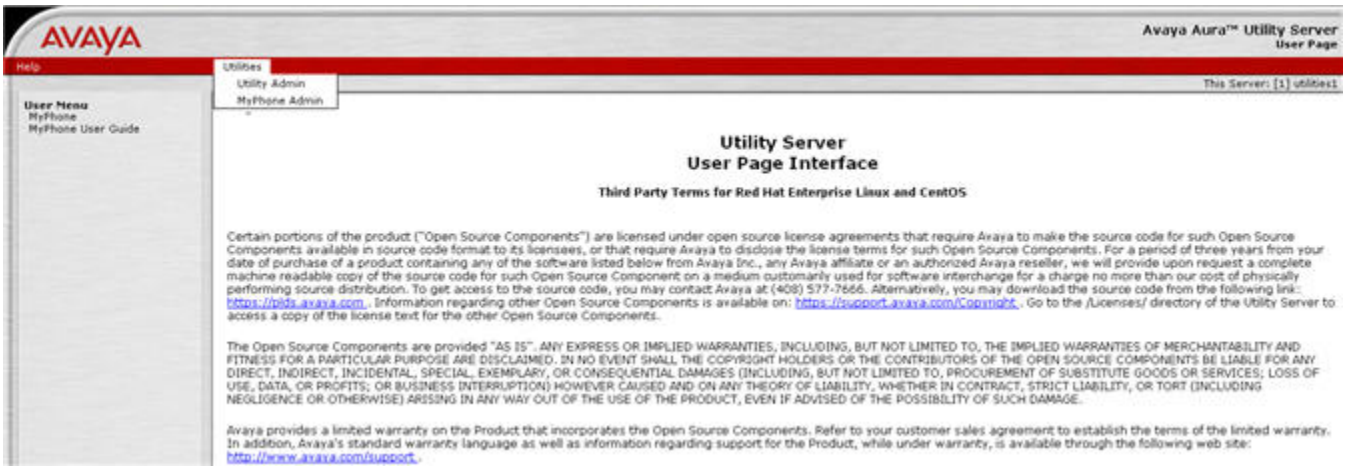
MyPhone

MyPhone enables you to configure the IP phones through a web interface. You can configure buttons, language settings, EC500, Enhanced Call forwarding and so on. It also enables you to change their station security codes and other parameters through the web interface.

MyPhone User Guide

MyPhone User Guide enables you to access the MyPhone documentation (a PDF file) without accessing the MyPhone application first.

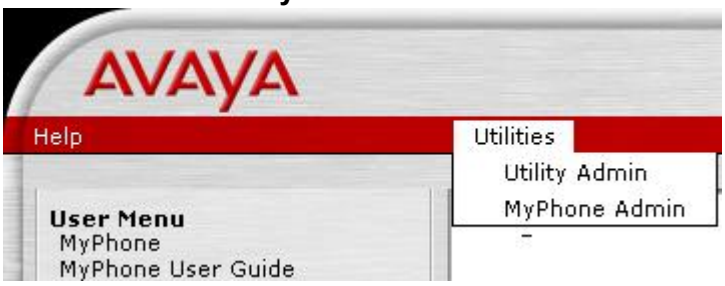
The Web-based management interface of the Utility Services is as follows:



Accessing Utility Services applications

The Utility Services administration web pages enable you to access various Utility Services applications and administer user settings and perform other administrative activities.

1. Enter the Utility Services URL on your web browser.
2. Click **Utilities** > **Utility Admin**.



3. Enter the user name.
4. Click **Logon**.
5. Enter the password.
6. Click **Logon**.

The system displays the Utility Services menu.

Telephony media modules

The Branch Gateway supports the MM711, MM714, MM714B, and MM716 analog media modules, the MM712 and MM717 DCP media modules, the MM710 E1/T1 media module, and the MM720 and MM722 BRI media modules.

Related topics:

MM711 analog media module on page 24
MM714 analog media module on page 25
MM714B analog media module on page 26
MM716 analog media module on page 26
MM712 DCP media module on page 27
MM717 DCP media module on page 27
MM710B E1/T1 media module on page 28
MM720 BRI media module on page 28
MM722 BRI media module on page 29

MM711 analog media module

The MM711 provides analog trunk and telephone features and functionality.

Related topics:

MM711 ports on page 24
Other MM711 features and functionality on page 25

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 (ringer equivalency number) for up to 2,000 feet (610 meters) for all eight ports
- 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.

Related topics:

MM714 ports on page 25
MM714 line ports on page 25
Other MM714 features and functionality on page 26

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 for up to 2,000 feet (610 meters) for all eight ports
- 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

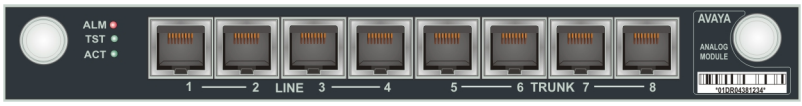


Figure 3: The MM714 media module

MM714B analog media module

The MM714B analog media module provides all the features provided by the MM714 (see MM714 analog media module on page 25), and in addition provides an emergency transfer relay.

Related topics:

MM714B and ETR on page 26

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.

Related topics:

MM716 ports on page 27

Other MM716 features and functionality on page 27

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 for up to 2,000 feet (610 meters) for all 24 ports
- Up to 24 simultaneously-ringing ports
- Type 1 caller ID
- Ring voltage generation for a variety of international frequencies and cadences

The MM716 is compatible with Avaya Aura®™ Communication Manager release 3.1 and higher, and Branch Gateway firmware version 29.x.x and higher.

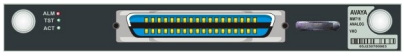


Figure 5: The MM716 media module

MM712 DCP media module

The MM712 DCP media module provides eight DCP telephone ports. The ports support two-wire Digital Communications Protocol (DCP) telephones. See Technical specifications on page 61 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.

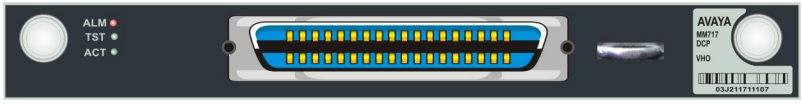


Figure 7: The MM717 media module

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

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 28.

Figure 10: The MM722 media module

Note:

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

WAN media modules

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

Related topics:

MM340 E1/T1 WAN media module on page 29
MM342 universal serial data WAN media module on page 30

MM340 E1/T1 WAN media module

Note:

The MM340 is no longer sold.

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

Figure 11: The MM340 media module

MM342 universal serial data WAN media module

Note:

The MM342 is no longer sold.

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

- V.35/ RS449
- X.21

Related topics:

Required cable on page 30

Required cable

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

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

Figure 12: The MM342 media module

Media module slot configurations

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

Related topics:

Permitted slots on page 31
G450 media module capacity on page 31

Permitted slots

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

Table 2: Permitted slots for media modules

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

G450 media module capacity

The G450 chassis is designed to accommodate:

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

Chapter 3: Summary of services

Summary of services

The Branch Gateway offers various services, which are described in Branch Gateway services on page 34, LAN services on page 41 and WAN services on page 43.

Related topics:

IPv6 on page 33
Branch Gateway services on page 34
Physical media on page 35
Media Gateway Controllers on page 37
Additional features on page 40

IPv6

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

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

Addressing

By using 128-bit addresses, IPv6 has about $3.4x10^{38}$ unique IP addresses, more than enough for every network device. This eliminates the IPv4 mechanisms, such as NAT (network address transitions), that are used to relieve IP address exhaustion. IPv6 addresses are normally written as hexadecimal digits with colon separators, for example: 2005:af0c:168d::752e:375:4020. The double colon "::" represents a string of zeroes, according to RFC4291.

Simplicity

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

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

- Routers no longer need to calculate the time a packet spent in a queue.
- IPv6 supports stateless address configuration, so IPv6 hosts can be configured automatically when connected to a routed IPv6 network through ICMPv6. Stateful configuration using DHCPv6 and static configuration are also available.

Deployment and transition

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

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

Key differences between IPv4 and IPv6

	IPv4	IPv6
Address space	32-bit, about $4.3x10^9$	128-bit, about $3.4x10^{38}$
Security	IPSec support is optional.	IPSec support is required.
Configuration	Requires DHCP or manual configuration.	Stateless auto-configuration. Does not require DHCP or manual configuration.
Address format	Decimal digits with colon separators, for example: 192.168.1.1	Hexadecimal digits with colon separators. For example: 2005:af0c:168d::752e:375:4020. The double colon "::" represents four zeros "0000"
Broadcast and Multicast support	Yes	No Broadcast. Various forms of Multicast — better network bandwidth efficiency
QoS support	ToS using DIFFServ	Flow labels and flow classes, more granular approach.

Feature Support in Avaya Branch Gateways

Certain Branch Gateway features are not supported in IPv6. See to the detailed feature information and Branch Gateway features

Branch Gateway services

The Branch Gateways provide a telephone exchange service, supporting the connection of various types of telephones and outside telephone lines. Telephones and lines are connected

to the Branch Gateways through media modules on the chassis. Different media modules provide access ports for different types of telephones and lines.

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

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

Related topics:

Voice over IP (VoIP) on page 35

Voice over IP (VoIP)

The Branch Gateway:

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

The Branch Gateway provides VoIP services over the LAN and WAN. The G450 supports up to four VoIP DSP childboards. Two types of childboard are supported, one providing 80 active VoIP channels and the other providing 20 active VoIP channels. The maximum number of active channels supported is 320. All channels can be bi-directional FAX, G.711 u/A, G. 726A, or G.729A/AB calls.

Physical media

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

Related topics:

Telephones on page 36
Voice software on page 36
Outside telephone lines on page 36

Telephones

The Branch Gateway supports IP telephones, Avaya DCP telephones, analog telephones, and BRI telephones. For information about which Avaya telephones are supported, see Supported Avaya telephones on page 59.

Telephones must be connected to the correct type of port for the telephone type. Different types of telephone ports are provided by different media modules. The table below lists which ports you can use to connect each type of telephone. See Optional components on page 19 for more information about each type of port and media module.

Table 3: Telephones supported and ports provided

Telephone type	Ports
IP telephones	An external LAN switch must be connected to one of the front panel ETH LAN ports. **Note:** The registration and signaling control information is under the direct control of the S8xxx server.
Avaya DCP digital telephones	DCP ports on the MM712 and MM717 media modules.
Analog telephones	Analog line ports on the MM711, MM714, MM714B, and MM716 analog media modules.

Voice software

The Branch Gateway supports telephone calls between a computer on the network running Avaya Softphone software and analog telephones connected to the Branch Gateway.

Outside telephone lines

The table below lists which modules you can use to connect each type of outside line. See Optional components on page 19 for more information about each type of port and media module.

Table 4: Outside telephone lines supported and ports provided

Line Type	Ports
ISDN line	ISDN ports on the MM720 and MM722 BRI media modules.
Analog trunks	Analog trunk ports on the MM714 or MM714B analog media module. Universal analog ports on MM711.

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

Media Gateway Controllers

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

An Avaya S8XXX server managed with Avaya Aura® Communication Manager (Communication Manager) software acts as an MGC for the Branch Gateway.

Related topics:

Supported S8XXX servers on page 37
Configuration rules for Branch Gateway options on page 38
Branch Gateway management on page 39
Avaya AuraCommunication Manager features on page 39
Avaya AuraCommunication Manager software applications on page 40

Supported S8XXX servers

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

Table 5: MGCs supported by the Branch Gateways

MGCs	Type	Usage
Avaya S8300D Server	Media module	ICC, ECC or LSP
Avaya S8800 Server	External	ECC
Dell R610	External	ECC

See Optional components on page 19 for information about the S8300D Server module.

Configuration rules for Branch Gateway options

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

- You can configure the Branch Gateway to use up to four MGCs, each controller can have one IPv4 and IPv6 address. If the MGC is an S8710, S8720, or S8730, the first server on the list is normally be the primary C-LAN board connected to the S8xxx server. If the MGC is an S8400 or S85XX, the first server on the list is either the primary C-LAN board connected to the S8xxx server or an Ethernet port on the server that you enabled for processor Ethernet connections. If the MGC is an S8300, the first server on the list is the IP address of the S8300. The remaining servers are alternate C-LAN boards connected to the S8xxx server (S8400, S85XX, or S87XX servers), an S8300 configured as an SRS, or the port enabled as the Ethernet processor port on an S85XX configured as an SRS.
- To maximize the capacity of a G450, you can configure an external Avaya S85XX Server installed on the local site as the primary MGC.
- Using the connection preserving migration feature, you can configure the Branch Gateway to preserve the bearer paths of stable calls if the Branch Gateway migrates to another MGC (including an SRS), including migration back from an SRS to the primary MGC. A call for which the talk path between parties in the call is established is considered stable. A call consisting of a user listening to announcements or music is not considered stable and is not preserved. Any change of state in the call prevents the call from being preserved. For example, putting a call on hold during MGC migration causes the call to be dropped. Special features, such as conference and transfer, are not available on preserved calls. Connection preserving migration preserves all types of bearer connects except BRI. PRI trunk connections are preserved.
- You can configure Standard Local Survivability (SLS) to enable a local Branch Gateway to provide a degree of MGC functionality when no link is available to an external MGC. You configure SLS from the Branch Gateway using the CLI. SLS is supported for all analog interfaces, ISDN BRI/PRI trunk interfaces, non-ISDN digital DS1 trunk interfaces (T1 Robbed Bit and E1-CAS), IP telephones, IP softphones, and DCP telephones. SLS is available on IPv4 only
- You can configure Enhanced Local Survivability (ELS) by installing an S8300 in the Branch Gateway as a Survivable Remote Server (SRS). In this configuration, the S8300 is not the primary MGC but takes over to provide continuous telephone service if all external MGCs become unavailable. Calls in progress continue without interruption when the S8300 takes over.
- You can configure the dialer interface to connect to the Branch Gateway's primary MGC by a serial modem if the connection between the Branch Gateway and the MGC is lost.
- You can configure Avaya Communication Manager to support the auto fallback feature, which enables an Branch Gateway being serviced by an SRS to return to the primary MGC automatically when the connection is restored between the Branch Gateway and the MGC. When the Branch Gateway is being served by the SRS, it automatically

attempts to register with the MGC at periodic intervals. The MGC can deny registration in cases in which it is overwhelmed with call processing, or in other configurable circumstances. By migrating the Branch Gateway to the MGC automatically, a fragmented network can be unified more quickly, without the need for human intervention.

Note:

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

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

Branch Gateway management

The Branch Gateway is managed by the Avaya Aura® Communication Manager (Communication Manager). The Branch Gateway supports Avaya Aura® Communication Manager (Communication Manager) release 6.x and is backwards compatible with release 5.0 and above.

Avaya Aura®Communication Manager features

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

- Telephony features
- Localization
- Collaboration
- Mobility
- Messaging
- Telecommuting
- System management
- Reliability
- Security, privacy, and safety
- Hospitality

- Attendant features
- Networking
- Intelligent call routing
- Application programming interfaces

Avaya Aura®Communication Manager software applications

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

For more information about Avaya Communication Manager software, see *Administrator's Guide for Avaya Aura® Communication Manager*.

Additional features

The Branch Gateway also provides voice-related features.

Related topics:

Call center capabilities on page 40
Emergency Transfer Relay (ETR) on page 41
Contact closure on page 41
Fax, modem, TTY over IP on page 41

Call center capabilities

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

Emergency Transfer Relay (ETR)

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

Contact closure

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

Fax, modem, TTY over IP

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

LAN services

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

Related topics:

LAN physical media on page 42
VLANs on page 42
Rapid Spanning Tree Protocol (RSTP) on page 42
Port mirroring on page 42
Port redundancy on page 43
Link Layer Discovery Protocol (LLDP) on page 43

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

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

Rapid Spanning Tree Protocol (RSTP)

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

Port mirroring

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

Port redundancy

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

Link Layer Discovery Protocol (LLDP)

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

LLDP is supported on the front panel ETH LAN ports.

WAN services

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

Note:
Certain WAN services are supported on IPv4 only.

Related topics:

WAN physical media on page 43
WAN features on page 44
Data and Routing features on page 46

WAN physical media

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

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

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

Related topics:

WAN line support on page 44
Media modules necessary for each WAN line on page 44

WAN line support

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

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

Media modules necessary for each WAN line

The table below lists which media modules to install to connect each type of outside WAN line. For more information about each type of media module, see Optional components on page 19.

Table 6: Outside WAN lines supported and matching media modules

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

WAN features

The Branch Gateway supports the following WAN features:

Note:

These features are only available on IPv4.

- Traffic shaping. The traffic shaping function estimates the parameters of the incoming traffic and takes action if it measures traffic exceeding agreed parameters. The action could be to drop the packets or mark them as being high drop priority.
- PPP over channeled and fractional E1/T1. The Branch Gateway has the ability to map several PPP sessions to a single E1/T1 interface.
- PPP over Universal Serial Port
- PPPoE
- Unframed E1 for enabling full 2.048 Mbps bandwidth usage
- Point-to-Point Frame Relay encapsulation over channelized/fractional/unframed E1/T1 ports or over a Universal Serial Port interface
- Frame Relay LMI types supported: ANSI (Annex D), ITU-T:Q-933 (Annex A0), LMI-Rev1, and No LMI
- Backup functionality supported between any type of Serial Layer 2 interface
- Dynamic Call Admission Control (CAC) for Fast Ethernet, Serial, and GRE tunnel interfaces. Dynamic CAC provides enhanced control over WAN bandwidth. When Dynamic CAC is enabled on an interface, the Branch Gateway informs the MGC of the actual bandwidth of the interface and tells the MGC to block calls when the bandwidth is exhausted.
- Quality of Service (QoS). The Branch Gateway uses Weighted Fair VoIP Queuing (WFVQ) as the default queuing mode for WAN interfaces. WFVQ combines weighted fair queuing (WFQ) for data streams and priority VoIP queuing to provide the real-time response time that is required for VoIP. The Branch Gateway also supports the VoIP Queue and Priority Queue legacy queuing methods.
- Weighted Random Early Detection (WRED). The Branch Gateway uses WRED on its ingress and egress queues to improve the performance of the network when overloaded. The purpose of WRED is to indicate to transmitting hosts to reduce their transmission speed when the ingress Branch Gateway queues are congested.
- Policy. Each interface on the Branch Gateway can have four active policy lists:
  - Ingress Access Control List
  - Ingress QoS List
  - Egress Access Control List
  - Egress QoS List

  Access control lists define which packets should be forwarded or denied access to the network. QoS lists change the DSCP and 802.1p priority of routed packets according to the packet characteristics.
- Policy-based routing. The Branch Gateway features policy-based routing, which uses a policy list structure to implement a routing scheme based on traffic source, destination, type, and other characteristics. You can use policy-based routing lists (PBR lists) to determine the routing of packets that match the rules defined in the list. Common

applications include separate routing for voice and data traffic, routing traffic originating from different sets of users through different Internet connections (Internet Service Providers), and defining backup routes for defined classes of traffic.

- RTP Header Compression. The Branch Gateway saves up to 60% of the bandwidth necessary using RTP compression. It also enhances the efficiency of voice transmission over the network by compressing the headers of Real Time Protocol (RTP) packets, thereby minimizing the overhead and the delays involved in RTP implementation.
- TCP Header Compression. The Branch Gateway uses Transmission Control Protocol (TCP) header compression to reduce the amount of bandwidth needed for non-voice data. TCP header compression can be applied either as part of RTP Header Compression via IPCH, or using the Van Jacobson method defined in RFC 1144.
- Inter-Gateway Alternate Routing (IGAR). The Branch Gateway uses IGAR as a means to use the PSTN as an alternative to the WAN interface under certain definable conditions. In providing an alternate routing mechanism, IGAR preserves the internal makeup of the call so that the call can be successfully terminated to its original internal destination.

Data and Routing features

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

Note:
Features labelled * are only available on IPv4.

- Interfaces*
- Routing table
- VPN
- GRE tunneling*
- DHCP and BOOTP relay*
- DHCP server
- DHCP client*
- Broadcast relay
- ARP table
- ICMP errors
- RIP*
- OSPF*
- Route redistribution
- VRRP*
- Fragmentation

- Static routes
- Policy-based routing*
- Distribution lists
- Dynamic IP addresses
- DNS resolver
- Unnumbered IP interfaces
- SYN cookies
- Keepalive packets
- Object tracking
- Backup interfaces

Chapter 4: Management, Security, Alarms and Troubleshooting

Management, Security, Alarms and Troubleshooting

Management applications

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

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

Related topics:

Branch Gateway Command Line Interface (CLI) on page 49
Avaya Branch Gateway Manager and Embedded Web Manager on page 50
Avaya Integrated Management on page 50

Branch Gateway Command Line Interface (CLI)

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

You can access the CLI with any of the following:

Note:
Telnet and the Services port are supported on IPv4 only.

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

Note:

Telnet is disabled by default on the Branch Gateway

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

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

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

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 *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.

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.

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 G450 Branch Gateway provides a comprehensive guide to configuring and using these solutions.

Related topics:

Front panel LEDs on page 52
Automatic error detection on page 52
SNMP on page 52
Packet sniffing on page 52
VoIP debugging using RTP-MIB on page 53

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 S8xxx 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 S8xxx 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 S8xxx server hard disk.

Chapter 5: Branch Gateway capacities

Branch Gateway capacities

G450 maximum Branch Gateway capacities

Table 7: G450 Branch Gateway capacities

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

Description	Capacity	Comments
Maximum number of analog phones per G450 Branch Gateway	192	
Maximum number of DCP phones G450 Branch Gateway	192	
Maximum number of BRI endpoints per G450 Branch Gateway	128	
Simultaneous two-way conversations with TDM transcoding from IP phone to legacy telephone or trunk.	206	
Simultaneous two-way conversations with TDM transcoding from TDM phones to IP phones	206	
Maximum number of BRI trunks	64	
Maximum number of PSTN trunks	184 (T1) 240 (E1)	For E1 trunks: 240 channels are supported in Tandem mode; 206 channels are supported for IP to PSTN
Miscellaneous		
Simultaneous fax transmissions	240	Fax transmissions using VoIP resources
Touch-tone recognition (TTR)	64	
Tone Generation	unlimited	
Announcements ports	63 ports for playback 1 for record	

S8300 maximum capacities

Table 8: S8300 capacities

Item	Quantity Supported
Number of Users per S8300	450
Number of Trunks per S8300	450
Total Endpoints (Trunks and Users) per S8300	900

Item	Quantity Supported
MGs per S8300	50
LSPs per S8300	49
MGs per LSP	50
Announcement Sources per S8300	50
Busy Hour Calls (Maximum, non-call center)	10,000
Locations	50

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

Chapter 6: 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 supports all Avaya IP telephones, including the Avaya 1602, 1608, and 1616 H.323 IP phones.

Avaya DCP digital telephones

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

- Avaya 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 8403 Digital Telephone
- Avaya 8405B and Avaya 8405D+ Digital Telephones
- Avaya 8410 and 8410D Digital Telephones
- Avaya 8411D Digital Telephone

- Avaya 8434DX Digital Telephone
- IP softphones that are configured as “Road Warrior” and “Take Over” a DCP station
- Definity Extender – Analog single endpoint
- Definity Extender – ISDN single endpoint 302 series Attendant Console (302D)
- Avaya 603E Call Master III
- Avaya 603F Call Master IV
- Avaya 607A Call Master V
- Avaya 606B1 Call Master VI
- Avaya eConsole R1 (PC Console R3 with 8411 digital telephone)
- Avaya IP eConsole

Avaya analog telephones

The Branch Gateway supports the following Avaya analog telephones:

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

Chapter 7: 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 9: Avaya G450 Branch Gateway specifications

Description	Value
Height	5.25 in. (3U, 133.3 mm)
Width	19 in. (482.6 mm)
Depth	18 in. (460 mm)
Weight of empty chassis	16.5 pounds (7.5 kg)
Weight of chassis with basic configuration, including main board, power supply unit, fan tray, one DSP, and blank panels on the media module slots	31 pounds (14 kg)
Ambient working temperature	32° to 104°F (0° to 40°C)
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	90-264 VAC, 47-63 Hz
BTU	1,780 BTU/h

Description	Value
Max current	7 A

Power cord specifications

For North America

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

For outside North America

The cord must be VDE Certified or Harmonized (HAR), rated 250V, 3-conductor (3rd wire ground), 1.0 mm2 minimum conductor size. The cord is to be terminated at one end to a VDE Certified/CE Marked IEC 60320, sheet C13 type connector rated 10A, 250V and the other end to a 3-conductor grounding type attachment plug rated at a minimum of 10A, 250V and a configuration specific for the region/country in which it will be used. The attachment plug must bear the safety agency certifications mark(s) for the region/country of installation.

Media module specifications

Table 10: Media modules

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

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

O

P

Q

R

S

T

U

V

W