



Job Aids for Field Replacement Units for the Avaya S8300D Server with G450 or G430 Branch Gateway

Release 6.2
03-300528
Issue 7
July 2012

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://support.avaya.com>.

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 may 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://support.avaya.com>. 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 IECCE 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:

A. 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

B. 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 matériel est conforme aux spécifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity



Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Européenne) 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>.

Contact Avaya Support

See the Avaya Support Web site: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support Web site: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.



Replacing the S8300D server or the S8300D server hard drive	7
Support.	7
Before you begin.	7
At the customer site	9
Replacing the S8300D server	10
Replacing the S8300D hard drive	11
Replacing the G450 or G430 branch gateway	17
Before you begin.	17
Before you go to the site	18
At the customer site	19
Appendix 1: Setting up a TFTP server	25
Appendix 2: Installing firmware using the TFTP server.	26
Replacing media and expansion modules	29
Replacing media modules.	29
Replacing the Avaya Media Modules.	30
Replacing Avaya Expansion Modules	31
Supported CD/DVD ROM drives	33
Types of CD/DVD ROM drives.	33
Panasonic Digistor	33
Sony	34
Addonics	34
Connecting the CD/DVD ROM drives to the server	34

Contents



Replacing the S8300D server or the S8300D server hard drive

This job aid describes the procedures to replace an installed S8300D server or the S8300D hard drive. For replacing the S8300A, S8300B and S8300C servers, see *Upgrading Avaya Aura® Communication Manager*, 03-603560.

The procedures in this job aid are applicable only to the replacement of the S8300D server running on either the CM_SurvRemote or CM_onlyEmbed template.

The term S8300 hardware refers to the S8300D server and its 250 GB hard disk drive. The material ID of the S8300D server is 700447675.

The Product Correction Notices are available at <http://support.avaya.com/>.

Support

Visit the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. On the Avaya Support website at <http://support.avaya.com>, search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to help answer questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Before you begin

1. Determine the configuration of the existing server.
If the existing server runs the CM_onlyEmbed template, determine if:
 - The server runs Communication Manager Messaging.

Replacing the S8300D server or the S8300D server hard drive

- Utility Server supports the phone firmware download function.

If the existing server runs the CM_SurvRemoteEmbed template, determine if it also runs Branch Session Manager.

Determine if Communication Manager has the Unicode (Phone Message) files installed.

If Utility Server supports phone firmware download function and the System Platform backup is unavailable, go to Step 2.

If the existing server utilizes Services VM with SAL gateway enabled and the System Platform backup is unavailable, go to Step 2.

2. Determine the backup files you will use in the S8300D server or S8300D hard drive procedure.

Check if backup files can be created. If they cannot be created, use the existing customer backup files.

Ensure that you have the customer backup server IP address and the account required to access the files.

The following are the preferred backup sets:

- System Platform.
- Communication Manager Messaging translations, names, and messages. This backup is applicable only to the CM_onlyEmbed template.
- Communication Manager Messaging announcements. This backup is applicable only to the CM_onlyEmbed template.

The following are the first alternatives to the preferred backup sets:

- Communication Manager full backup or backup of translation files.
 - Utility Server backup.
 - Communication Manager Messaging translations, names, and messages. This backup is applicable only to the CM_onlyEmbed template.
 - Communication Manager Messaging announcements. This backup is applicable only to the CM_onlyEmbed template.
3. If the existing server is functional, perform the System Platform backup which contains the server configuration for System Platform, Communication Manager, BSM and Utility Server. The System Platform backup does not contain the server configuration for Communication Manager Messaging.
 4. If the existing server is functional, perform Communication Manager Messaging backup.
 5. Ensure that you have the software versions for the following:
 - Avaya Aura[®] System Platform
 - Avaya Aura[®] Communication Manager
 - Communication Manager Messaging

- Services VM
 - Utility Server
 - BSM
6. Download the current license file and authentication file from the PLDS Web site. The license file must be associated with the serial number of the gateway in which the defective hardware resides. Save the license and authentication files on the laptop that you will use at the customer site. For the replacement of the hard drive, use the license file that has been generated by the system.
 7. Determine whether software service packs and firmware files are required. If the service pack is required, download the service pack and save it on your laptop.

At the customer site

1. If the hardware is functional, connect your laptop to the services port on the server. Then, on the **System Platform** home page, select **cdom** and click **Server Management**.

If the system does not display the **System Platform** home page, perform the following steps to determine if the hardware is functional:

- a. Connect the customer laptop with a crossover cable to the services port on the server, and go to the **System Platform** home page.
- b. If you do not get the **System Platform** home page, unplug and replug the power cord, and try navigating to the page again. If you still face problems while gaining access to the page, then the hardware is not functional. See [Replacing the S8300D server](#) on page 10.

**WARNING:**

Turning the server off can cause service outage.

2. Back up data:
 - a. On the **System Platform** home page, click **Server Management > Backup/Restore > Backup**.
 - b. On the **Backup** screen, click the **Backup** tab.
 - c. Click **Backup Now**.
 - d. Select SFTP as the backup method and enter the following customer information:
 - User Name
 - Password
 - Host Name
 - Directory

- e. Click **Backup Now**.

Note:

You must take a complete backup of the system, including Communication Manager Messaging, if installed.

Replacing the S8300D server

1. Shut down the server using either the Web interface or the **Shutdown** button on the server faceplate.
 - On the **System Platform** home page, click **Server Management > Server Reboot/Shutdown**. Click **Shutdown Server**.
 - Alternatively, press the **Shutdown** button on the server faceplate. Hold the button until the green **OK to Remove** LED starts blinking.
2. When the **OK to Remove** LED is steady, loosen the two thumb screws on the server.
3. Remove the S8300D server.
4. Connect the USB CD/DVD drive to the server. Insert the System Platform software media.
5. Completely insert the server in the gateway slot and secure the server faceplate with the thumb screws. Tighten the thumb screws.
6. Turn on the gateway if you had turned it off earlier.
7. Connect your laptop to the services port on the server.
8. Install System Platform from the DVD.

The server reboots after installation.
9. If required, install the System Platform patches and the Services VM patches.
10. Use the services laptop or a network connection to gain access to the **System Platform** home page.
11. Enter the configuration data into the server during template installation.
12. If the server is configured as Main Server, install the CM_onlyEmbed template.

If the server is configured as Survivable Remote Server, install the CM_SurvRemoteEmbed template.
13. If required, install the Communication Manager service pack, the BSM service pack and patch, and the Utility Server service pack.
14. If the System Platform backup is available:
 - a. Restore the System Platform data.
 - b. If the S8300D server was replaced, you must install an updated license file and authentication file. If you replaced the disk and are reusing the S8300D server, you do not need to reinstall the license and authentication file.

15. If the System Platform backup is unavailable and you have a Communication Manager backup:
 - a. Configure Communication Manager as you would configure a new installation.
 - b. Restore the Communication Manager data.
 - c. Reboot the Communication Manager virtual machine by using the Communication Manager Web page and clicking **Shutdown Server** or the System Platform Webconsole Web page and clicking **Manage**.
16. If required, install the Communication Manager Messaging service pack.
17. If required, restore the Communication Manager Messaging data that includes translations, names, and messages.
18. If required, restore the Communication Manager Messaging announcements.
19. Start Communication Manager Messaging.
20. If required, install Communication Manager Unicode (phone messages) file.
21. Check for any new alarm and resolve the alarm.
22. Test as appropriate. For example, make station and trunk calls.
23. Save the translations files. If the server on which you replaced the hardware is configured as a survivable remote server, save the translations files on the primary controller and not on the survivable remote server.
24. Activate alarm origination.
 - a. At the server command line, type **almenable -d b -s y** and press **Enter**.
 - b. Type **almenable** without any options and press **Enter** to verify that alarm origination is active.
25. Log off from the system.

Replacing the S8300D hard drive



CAUTION:

Ensure that you wear a properly grounded ESD wrist strap while handling the server hard drive. Place all components on a grounded, static-free surface while working on them. Hold the hard drive by the edges. Do not touch the bottom of the hard drive.

1. Shut down the server using either the Web interface or the Shutdown button on the server faceplate.
 - On the **System Platform** home page, click **Server Management > Server Reboot/Shutdown**. Click **Shutdown Server**.

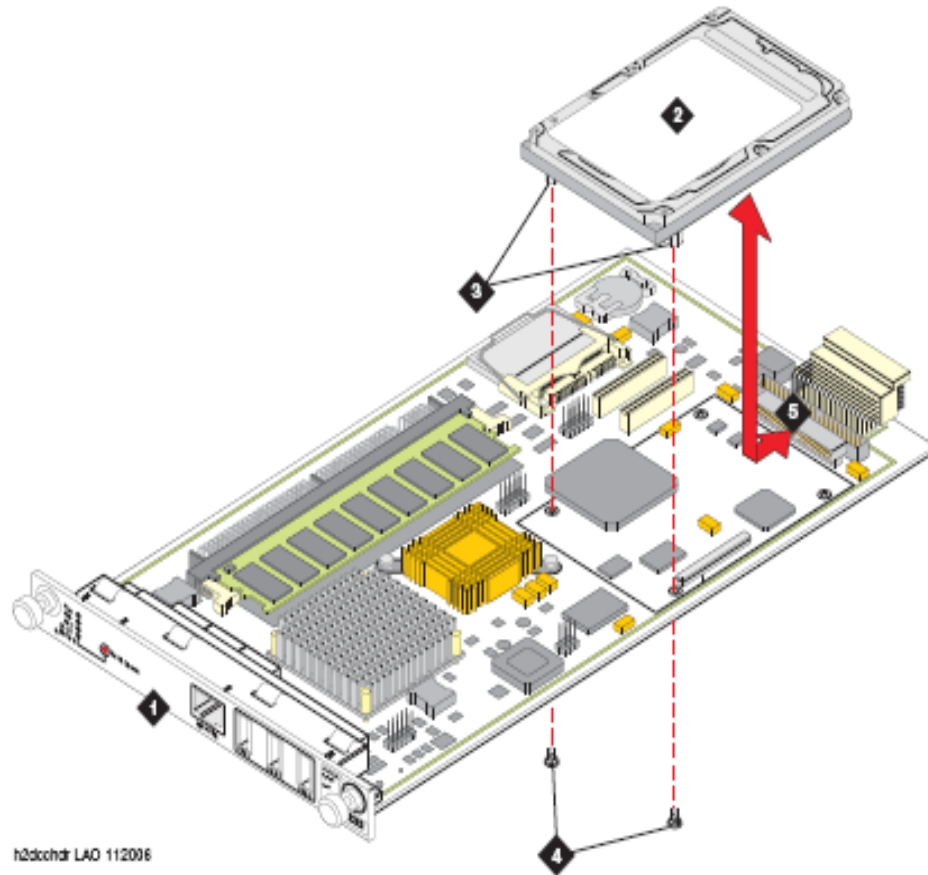
Replacing the S8300D server or the S8300D server hard drive

- Alternatively, press the **Shutdown** button on the server faceplate. Hold the button until the green **OK to Remove** LED starts blinking.
- 2. When the **OK to Remove** LED is steady, loosen the two thumb screws on the server.
- 3. Remove the S8300D server.

Note:

If standoffs are not included with the new hard drive, remove the standoffs from the old hard drive and reuse them. Before screwing the standoffs into the new hard drive, clean the threads thoroughly with a damp cloth or paper towel.

- a. From the server, remove the two screws that are attached to the hard drive standoffs. See [S8300D hard drive replacement](#).

Figure 1: S8300D hard drive replacement**Figure notes:**

1. S8300D server
2. Hard drive
3. Hard drive standoffs
4. Hard drive mounting screws (2)
5. Hard drive connector

-
- b. Detach the hard drive by pulling it out of the connector.
 - c. Locate the standoffs for the new hard drive. If standoffs are not included in the new hard drive, remove the standoffs from the old drive and reuse them.
 - d. Screw the standoffs into the new hard drive.
 - e. Connect the hard drive to the hard drive connector.
 - f. Align the hard drive standoffs with the mounting holes on the server.
 - g. Hold the server by its side, with the hard drive aligned with the mounting holes, and attach the server to the hard drive standoffs.

Replacing the S8300D server or the S8300D server hard drive

- h. Insert the server into the appropriate slot of the gateway. For example, use slot V1 of the G450 or G430. Do not completely insert the server in the slot.
4. Before completely inserting the server into the appropriate slot of the gateway, connect the USB CD/DVD drive to the server. Insert the System Platform software media.
5. Completely insert the server in the gateway slot and secure the server faceplate with the thumb screws. Tighten the thumb screws.
6. Turn on the gateway if you had turned it off earlier.
7. Connect your laptop to the services port on the server.
8. Install System Platform from the DVD.

The server reboots after installation.
9. If required, install the System Platform patches and Services VM patches.
10. Use the services laptop or a network connection to gain access to the **System Platform** home page.
11. Enter the configuration data into the server during template installation.
12. If the server is configured as Main Server, install the CM_onlyEmbed template.

If the server is configured as Survivable Remote Server, install the CM_SurvRemoteEmbed template.
13. If required, install the Communication Manager service pack, the BSM service pack and patch, and the Utility Server service pack.
14. If the System Platform backup is available:
 - a. Restore the System Platform data.
 - b. If the S8300D server was replaced, you must install an updated license file and authentication file. If you replaced the disk and are reusing the S8300D server, you do not have to reinstall the license and authentication file.
15. If the System Platform backup is unavailable:
 - a. Configure Communication Manager as you would configure a new installation.
 - b. Restore the Communication Manager data.
 - c. Reboot the Communication Manager virtual machine by using the Communication Manager Web page and clicking **Shutdown Server** or the System Platform Webconsole Web page and clicking **Manage**.
16. If required, install the Communication Manager Messaging service pack.
17. If required, restore the Communication Manager Messaging data that includes translations, names, and messages.
18. If required, restore the Communication Manager Messaging announcements.
19. Start Communication Manager Messaging.
20. If required, install Communication Manager Unicode (phone messages) file.

21. Check for any new alarm and resolve the alarm.
22. Test as appropriate. For example, make station and trunk calls.
23. Save the translations files. If the server on which you replaced the hardware is configured as a survivable remote server, save the translations files on the primary controller and not on the survivable remote server.
24. Activate alarm origination.
 - a. At the server command line, type **almenable -d b -s y** and press **Enter**.
 - b. Type **almenable** without any options and press **Enter** to verify that alarm origination is active.
25. Log off from the system.

Replacing the S8300D server or the S8300D server hard drive



Replacing the G450 or G430 branch gateway

This job aid applies to G450 and G430 branch gateways only. For the G700, G250, and G350 media gateways, see the following documents:

- *Installing and Upgrading the Avaya G700 Media Gateway*, 03-603333
- *Installing and Upgrading the Avaya G250 Media Gateway*, 03-300434
- *Installing and Upgrading the Avaya G350 Media Gateway*, 03-300394

Replacement of a G450 or G430 branch gateway depends on the following scenarios:

1. You cannot log in to the gateway.
2. The gateway does not register with its primary controller.
3. The gateway reboots repeatedly.
4. The VoIP module on the gateway motherboard does not work.

This job aid describes the procedures to replace an existing G450 or G430 branch gateway with a new G450 or G430 branch gateway. The procedures depend on the following two considerations:

- The G450 or G430 branch gateway might include the S8300D server, which can be configured as a primary controller or as a survivable remote server.
- The G450 or G430 branch gateway might be functional.

Before you begin

Ensure that:

- An installed S8300D server and any installed media modules are reused in the new branch gateway.
- The customer-provided LAN is available to connect to:
 - The primary controller of the branch gateway if the primary controller is remote
 - The TFTP server support for the backup of the branch gateway configuration and .dat files, and installation of new firmware

Note:

You can use the Utility server application on System Platform for staging gateway firmware installation . See [Appendix 2: Installing firmware using the TFTP server](#) on page 26.

- The FTP server to back up the branch gateway VAL announcements

Replacing the G450 or G430 branch gateway

- The Branch Gateway Processor configurations are valid. This means that the IP addresses on the customer LAN are still available for the following:
 - Branch Gateway Processor (BGP)
 - VoIP engine on the branch gateway motherboard (voip-v0)
 - Primary controller (S8300D, S8510, S8800, HP or Dell server)
 - Survivable remote servers
 - FTP and TFTP server
- The Avaya Gateway Installation Wizard can be used for the initial configuration of the new branch gateway as well as the upgrade of firmware. The Gateway Installation Wizard application must be installed on the laptop of the technician.
- The technician is familiar with the procedures to connect and gain access to the G450 or G430 branch gateway and the S8300D server.

Before you go to the site

Perform the following procedure before going to the customer site:

1. Obtain the IP addresses of the primary controller and the survivable remote servers in the network. The primary controller can be an S8300D, an S8510, an S8800, an HP or a Dell server.
2. Obtain the IP addresses and subnet masks for the Branch Gateway Processor (BGP) on the branch gateway to be replaced and the default gateway IP address on the LAN of the customer.

Note:

Do not confuse the default gateway IP address with the BGP IP address.

3. Obtain the IP address of a computer on the customer LAN that must be set up as a TFTP server. The software required to set up a TFTP server can be downloaded from the Avaya Support Web site. Instructions to set up a TFTP server are given in [Appendix 1: Setting up a TFTP server](#).

You require the TFTP server for TFTP backups.

4. Check which media modules are installed on the branch gateway. You can obtain the information from the branch gateway itself. Alternatively, you can log in to the SAT interface of the primary controller and run the **display media-gateway number** command.
5. Download the most recent versions of firmware for each device in the branch gateway, including the BGP and the media modules, and save them on your laptop.

**CAUTION:**

The branch gateway or media module firmware must be compatible with the version of the Avaya Aura® Communication Manager software on the primary controller.

6. Obtain access to the primary controller.
 - If the primary controller is the S8300D server in the G450 or G430 branch gateway, use a direct connection from the NIC card of your laptop to the services port on the server. For example, you can configure your laptop with the static IP address 192.11.13.5.
 - If the primary controller is at a remote location, gain access to the primary controller over the LAN. The customer should provide a computer connected to the LAN for this purpose. Alternatively, you can contact someone who has access to the primary controller and ask the contact person to administer a new serial number on the **change media-gateway** <gateway number> SAT screen of the primary controller.

At the customer site

You must use your laptop to gain access to the branch gateway through a direct serial connection and the primary controller through a direct connection or over the LAN. You have to alternate between these two connections several times.

Perform the following procedures at the customer site:

1. Set up connections to the branch gateway, primary controller, and survivable remote server:
 - a. If the branch gateway is functional, connect your laptop to the console port on the branch gateway with a serial cable.
 - b. Connect to the primary controller:
 - If the primary controller is local, connect your laptop to the services port on the server with a crossover cable.
 - If the primary controller is at a remote location, connect LAN to the primary controller on the customer computer.

Note:

If the primary controller is an S8510, an S8800, an HP or a Dell server on a G450 or G430 branch gateway that is not being replaced, do not save translations at this point.

2. If the primary controller is an S8300D server and the branch gateway has to be replaced, save translations by using the SAT interface. Verify that translations are saved successfully.

Replacing the G450 or G430 branch gateway

Note:

If the branch gateway is not functioning, go to Step 6.

3. Back up the branch gateway configuration files to a TFTP server. The TFTP server must be on customer LAN, and the branch gateway must be connected to the LAN through one of the Ethernet ports, EXT1 or EXT2.
 - a. To open the SSH interface to the branch gateway, log in with your user name and password. The user name and password are provided by the system administrator.
 - b. At the CLI prompt, type **copy running-config tftp**.
4. Back up the branch gateway VAL announcements if gateway announcements are present on the branch gateway.

Note:

To determine if VAL announcements are present, log in to the SAT command line interface on the primary server, and type the command **list directory board <xx>v9**, where <xx> is the number of the branch gateway.

- a. To enable the file system, connect to the primary server and start a SAT session.
- b. Type **enable filexfer** and press **Enter**.
- c. On the Enable File Transfer screen, enter your login and password. The login must

```
enable filexfer                                     Page 1 of 1

                                     ENABLE FILE TRANSFER

                                     Login:
                                     Password:
Reenter Password:
                                     Secure?
Board address:
```

contain three to six alphanumeric characters, and the password must contain seven to eleven characters and at least one number.

- d. In the **Reenter Password** field, type the same password you created in Step c.
- e. In the **Secure** field, type **n** for FTP and **y** for SFTP.
- f. In the **Board address** field, type **<nnn>v9**, where **<nnn>** is the administered branch gateway number.
- g. Log in to a computer connected to the customer LAN. Use this computer as an FTP client to temporarily store the VAL announcements.
- h. Copy the existing announcement files from the branch gateway to the FTP client.

- Type
ftp <ip-address>
where **<ip-address>** is the IP address of the BGP on the branch gateway.
- Type the ftp username you created in Step a.
- Type the ftp password you created in Step a.
- Type **bin** to change to binary mode.
- Type **dir** to view the contents of the /annc directory.
- Type
get <filename>.wav
where **<filename>** is the file name of an announcement file that you want to back up.

Note:

The **get** command copies the announcement file to the directory from where you initiated the FTP session on the FTP client.

- Repeat the **get** command for each announcement file you want to back up.
 - i. Type **bye** to close the FTP session.
5. Ensure that all cables connected to the branch gateway and media modules are adequately marked for later reinstallation in the same location.
 6. Turn off the server and the branch gateway.
 7. Remove the old branch gateway from the rack and insert the new branch gateway.
 8. Transfer the media modules and the server from the old branch gateway to the new branch gateway, maintaining the original slot locations.
 9. Reconnect cables in the same location.
 10. To configure basic branch gateway connectivity:
 - a. Set up a laptop with SSH client software.
 - b. Set the TCP/IP properties of the laptop as follows:
 - Enter 192.11.13.5 in the **IP address** field.
 - Enter 255.255.255.252 in the **Subnet mask** field.
 - Disable **DNS service**.
 - Disable **WINS Resolution**.
 - c. Use an Ethernet cable to connect the laptop to the branch gateway services port.
 - d. SSH to 192.11.13.6.
 - e. At the prompt, enter root as the default username and rootroot0 as the default password.

Replacing the G450 or G430 branch gateway

- f. Configure a new password.
- g. At the prompt, enter **y** to configure basic gateway connectivity.

Note:

You can use the **script-config** CLI command to run the installation script if you have not saved any configuration changes.

- h. You will be prompted to configure the following parameters. For each parameter, leave the default value or enter a new value.
 - VLAN number
 - IPv4 enabled or disabled
 - IPv4 address for the primary management interface
 - IPv4 subnet mask for the primary management interface
 - IPv4 address for the default gateway (router)
 - IPv6 enabled or disabled
 - IPv6 unicast global address
 - IPv6 prefix length
 - IPv6 link local address
 - IPv6 PMI (Global or Link Local)
 - IPv6 default gateway
 - Eight IP addresses (four IPv4 and four IPv6) to specify the media gateway controllers
 - Hostname for the branch gateway

The system displays the settings you configured and the confirmation dialog box.

- If you confirm the settings, the settings are saved and the branch gateway reboots.
 - If you do not confirm the settings, the system prompts to reconfigure the parameters. If you enter **y**, the system displays the parameters again for configuration.
- i. To enable remote access to the gateway, connect the Ethernet port to the network.
11. To restore the configuration backup files:
 - a. At the MGP prompt, type **copy tftp start-up config**.
 - b. To check the status, type **show download status**.
 - c. To reset the BGP, type **reset**.
 12. To assign IP addresses to VoIP resources:

- a. Type **set interface voip <number> <ip address>**

where **<number>** is the slot number of the VoIP media module. The slot v0 designates the VoIP resource resident on the branch gateway motherboard. The MM760 VoIP Media Modules are designated according to the slot. For example, slots v1, v2, v3, and v4 are the slots in which the media module has been installed. **<ip address>** is the IP address of the VoIP resource. For example: **set interface voip v0 132.236.73.3**

13. To assign the controller list for the branch gateway if the existing branch gateway is not functional:

- a. Type the following commands to designate the primary, secondary, and survivable remote server controllers for the branch gateway:

clear mgc list

set mgc list <ip_address> [, <ip_address> [, <ip_address> [, <ip_address>]]]

where, the first **<ip_address>** is the IP address of the primary controller for the branch gateway.

Note:

To change the mgc list, run **clear mgc list** before you designate the primary, secondary, and survivable remote server controllers.

The following table describes the possible alternate controllers for an S8300, S8500, S8700, and S8710 primary controller:

Primary server	Controller IP addresses
S8300D	First: The IP address of the S8300D primary controller. Next three: One, two, or three IP addresses of the S8300D servers configured as survivable remote servers.
S8510, S8800, HP, or Dell	First: The IP address of the C-LAN/PE for the S8500, S8700, or S8710 primary controller. Next three: One, two, or three IP addresses of alternate C-LANs or survivable remote servers or both.

14. Set the survivable remote server transition points if the existing branch gateway is not functional.

If a network problem occurs:

- a. Type **set mgp reset-times primary-search <search-time>**

where **<search-time>** is the time in minutes that the branch gateway searches for a primary controller before looking for a survivable remote server. You can enter 1 through 60 minutes.

Replacing the G450 or G430 branch gateway

- b. Type **set mgp reset-times total-search <search-time>**
where **<search-time>** is the time in minutes that the branch gateway searches for both primary controllers or survivable remote servers. You can enter 1 through 60 minutes.
 - c. Type **set mgp reset-times transition-point <#_of_primary>**
where **<#_of_primary>** is the number of primary controllers in the controller list. If the primary controller is an S8510 or S8800 server, the range is from 1 through 4. If the primary controller is an S8300, **<#_of_primary>** must be 1.
15. Reconnect to the primary server.
16. To restore the announcement files:
 - a. Repeat Step a in Step 4 to enable an FTP session on the server.
 - b. Copy the backed-up announcement files from the FTP client to the branch gateway.
 - Type **ftp <ip-address>**
where **<ip-address>** is the IP address of the BGP.
 - Type the ftp-user name.
 - Type the ftp-password.
 - Type **bin** to change to binary mode.
 - Type **dir** to view the contents of the /annc directory.
 - Type **put <filename>.wav**
where **<filename>** is the name of an announcement file you want to restore.
 - c. Type **bye** to close the FTP session.
17. Reconnect to the branch gateway.
18. Determine which firmware to install on the branch gateway.

Compare software versions running on the branch gateway processors and media modules with the versions that you downloaded from the Avaya support Web site. If the versions do not match, installing new firmware for those components is necessary.
19. Install new firmware as appropriate.

You can use the server to stage the firmware. See [Appendix 2: Installing firmware using the TFTP server](#).

If you cannot use the TFTP server to stage the firmware, configure a TFTP server on a PC connected to the customer LAN. See [Appendix 1: Setting up a TFTP server](#).

20. Provision the new branch gateway.
 - a. On the primary controller, open a SAT session.
 - b. Type **change media-gateway <mg-number>**
where **<mg-number>** is the number assigned to this G700.
 - c. Type the serial number of the new branch gateway in the **Identifier** field and click **Submit**.
 - d. Verify that the new branch gateway registers with Communication Manager:
 - Open a SAT session and type **list media-gateway**.
 The **Registered?** column must display **y** for the new branch gateway.
21. Save translations on the primary controller.
22. Test as appropriate. For example, make station calls from or to the replaced branch gateway, check for and resolve any new alarms.

Appendix 1: Setting up a TFTP server

The following instructions describe how to configure a Windows-based computer as a TFTP server. A TFTP server is needed for the **copy tftp** commands, which back up the configuration files and install firmware on the branch gateway. The TFTP server can be on any computer that can be networked to a branch gateway.

Perform the following steps to configure a computer as a TFTP server:

1. Create a directory in which you will copy the branch gateway configuration files or load the firmware image files. For example, C:\tftpboot.
2. Go to <http://support.avaya.com/> and select **Downloads**.
3. Select **4600 Series IP Telephones**.
4. Scroll down the list of Software Downloads to recent posting. For example, **4601/... IP Telephone Release 111004 and TFTP Server (November 2004)**.
5. Search for **iptel_avaya_tftp.exe**.
6. Click the program and download it.

Download the **iptel.pdf** file, which provides instructions on installing iptel_avaya_tftp.exe on Windows systems.
7. Go to the directory containing the **iptel_avaya_tftp.exe** file. Double-click the file name and follow the installation wizard instructions to install the file.

The default installation directory is *c:\Program Files\Walusoft\TFTPSuite*. You can change the default installation directory.

8. Go to the directory where the TFTP software is installed and double-click the program **tftpserver32.exe**.

The system displays the **TFTP Server** screen. The upper section of the screen displays the IP address of the computer and port 69.

9. Enable the TFTP server as follows:
 - a. Click **System** from the Menu bar and select **Setup**.
The system displays the **server option** screen.
 - b. Click the **Outbound** tab and enter the path to the location of the tftp directory that you created in the **Outbound file path** screen.
 - c. Click the **Inbound** tab and enter the path of the tftp directory that you created in the **Inbound file path** screen.
 - d. In the **Options** tab, enter **69** in the **Use Port** field.
 - e. Select **No Incoming**. However, to copy files as a backup prior to performing an upgrade of software, do not select this field.
 - f. Click **OK**.

Note:

To use the TFTP server, double-click the program **tftpserver32.exe**. In the File menu, select **Start Serving**. You can turn the program off by selecting **Stop Serving**.

Appendix 2: Installing firmware using the TFTP server

The TFTP server is used to install firmware files on media gateways and media modules. For the latest firmware files for media gateways and media modules, go to <http://support.avaya.com>.

To install firmware files, you must use the TFTP server capability of Utility Server. Utility Server is available in all CM templates other than CM_Duplex.

1. On the **Utility Server** Web console, click **Utilities > Utility Admin**.
2. In the left navigation pane of the **Utility Admin** page, click **Upload Gateway firmware > Display Firmware Directory**. The system displays the firmware versions that are available on Utility Server.
3. If the required firmware version is unavailable on Utility Server, download the firmware file from the Web.
4. In the left navigation pane of the **Utility Admin** page, click **Miscellaneous > Upload Files**.
5. Browse to the downloaded firmware file and select it.

6. Click **Upload File**. The file is uploaded to Utility Server.
7. Check the **Display Server Firmware** page to ensure that the firmware file is uploaded.

Replacing the G450 or G430 branch gateway



Replacing media and expansion modules

This job aid applies to the S8300D server and the G450 or G430 branch gateway only. The procedures described in this job aid are as follows:

- [Replacing media modules](#)
- [Replacing Avaya Expansion Modules](#)

The Product Correction Notices are available at <http://support.avaya.com>.

Replacing media modules

[Table 1](#) lists the necessary information that you require to order and replace the media modules.

Table 1: Equipment List: Media Modules

Media Modules	
T1/E1 Media Modules	
Material Code	170900
Apparatus Code	MM710
Material ID (required for Maintenance Ordering only)	700221161R
DEF DS1 Loopback Jack 700A (used for remotely troubleshooting the T1/E1 Media Modules)	
Material Code	107988867R
Apparatus Code	None
DCP Media Module	
Material Code	170898
Apparatus Code	MM712
Material ID (required for Maintenance Ordering only)	700221153R
BRI Media Module	
Material Code	170898
Apparatus Code	MM720

Replacing media and expansion modules

Media Modules	
Material ID (required for Maintenance Ordering only)	700221138R
Analog Station/Trunk Module	
Material Code	170899
Apparatus Code	MM711
Material ID (required for Maintenance Ordering only)	700221146R

A media module needs to be replaced in case of:

- A damaged media module
- A change in the media module type

The modules on the branch gateway are not inserted until the branch gateway registers with Avaya Aura® Communication Manager. Similarly, all media modules and the associated maintenance objects are removed if the branch gateway link stops working. The term board insertion process refers to the process in which the media modules are queried for their type, suffix, and vintage. Use the **list config all** and the **list config media-gateway number** commands to obtain this information. Any media module that does not agree with administration generates a process error and is flagged to the relevant administration screen. The removal of the media modules is detected. Branch gateway circuit packs list the relevant slot location as no board. You can download the T1/E1 modes of operation for the DS1 media modules because the DS1 media module can function as either a T1 or an E1 interface.

After replacing the media module, the modules are registered with the branch gateway, where board type, suffix, and vintage are verified. The branch gateway then sends H.248 messages to the controller and creates Communication Manager objects.



CAUTION:

Be careful while aligning and inserting the connector pins.



CAUTION:

Separate the ESD paths to the chassis ground connected to the media modules at the spring-loaded captive screws. Ensure that the captive screws are securely tightened to prevent damage to the equipment.

Replacing the Avaya Media Modules

1. Identify and mark all cables.
2. Remove the cables.

3. Loosen the captive screws and slide out the old media module.
4. Position the media module squarely before the selected slot on the front of the branch gateway chassis and engage both the sides of the module in the interior guides.
5. Slide the module slowly into the chassis. Maintain an even pressure and ensure that the module does not twist or misalign. See [Figure 2: Inserting Media Modules](#) on page 31.
6. Apply firm pressure to engage the connectors.

The media module connector has pins of varying lengths. The long pins engage first to provide grounding. The medium length and short pins provide power and signal.

7. Lock the media module into the chassis by tightening the spring-loaded captive screws on the front of the module.
8. Plug in the cables in the correct order.

**WARNING:**

To prevent electrical hazards and to ensure continued compliance to international radiated emissions requirements, all captive screws must be securely tightened such that they cannot be loosened without the use of a tool.

Figure 2: Inserting Media Modules



Replacing Avaya Expansion Modules

You can optionally extend the G430 by attaching one or two EM200 expansion modules to the branch gateway. Since the cables attaching the EM200 expansion modules to the branch gateway are short, you must install the branch gateway and the expansion modules directly above or below each other. For more information on the EM200 expansion module, see *Installation and Upgrades for the Avaya Branch Gateway G430*, 03-603233.



Supported CD/DVD ROM drives

This job aid describes the supported CD/DVD ROM drives that technicians must use to install software on the Avaya S8300D server. The Product Correction Notices are available at the Avaya Support Web site.

This job aid includes the following topics:

- [Types of CD/DVD ROM drives](#)
- [Connecting the CD/DVD ROM drives to the server](#)

Types of CD/DVD ROM drives

The CD/DVD ROM drives supported on the S8300D server are:

[Panasonic Digistor](#)

[Sony](#)

[Addonics](#)

Panasonic Digistor

You can purchase Avaya-approved Panasonic Digistor models 73082 or 73322 (Comcode: 700406267).

Instead of AC power, the Panasonic Digistor drive use lithium-ion battery for additional power. USB 2.0 readers draw more power than the standard USB ports from the S8300D server. The Digistor drive contains an internal lithium-ion battery that makes up the current difference between what the USB port can provide and what the CD/DVD ROM drive requires.

Ensure that the internal lithium-ion battery is fully charged for the drive to operate properly. When the lithium-ion battery is depleted and the drive attempts to operate, the red LED on the case turns on and the screen displays the failed to mount cdrom message. The red LED is not bright so careful observation is required. The lithium-ion battery can be charged by plugging the CD/DVD ROM drive in a USB port for approximately 30 minutes. The lithium-ion battery charges faster if the ON/OFF switch is OFF. To preserve the battery, keep the ON/OFF switch in the OFF position until you are ready to use the Digistor drive.

Note:

The functionality of the internal lithium-ion battery charging the drive is only applicable with the original CD/DVD ROM drive.

Sony

The DRX-S70U-W model of SONY CD/DVD rewritable drive is unavailable through Avaya. The drive requires 5.2 V DC and comes with an AC power adapter.

Addonics

The AEPDVRWII824 model of Addonics CD/DVD reader is unavailable through Avaya. You must place the CD/DVD ROM drive on a surface within 5 degrees of level. The Addonics CD/DVD reader requires AC power to operate. You must set the power switch to EXT for the CD/DVD reader to operate.

Connecting the CD/DVD ROM drives to the server

To connect the CD/DVD ROM drive to an S8300 server:

1. On an Addonics drive, plug one end of the power cord into the drive and the other end into an electrical outlet.
2. Set the power switch to EXT (Addonics) or to ON (Panasonic).
3. Connect the USB cable to the USB port on the server faceplate and the other end of the USB cable to the CD/DVD drive.
4. Place the media into the external CD/DVD drive.