Avaya Aura® Communication Manager Change Description for Release 5.2.1

03-603443
Issue 2
January 2011

Notice

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

Documentation disclaimer

Avaya shall not be 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. 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 End User.

Link disclaimer

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

Warranty

Avaya 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 to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

- Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the

Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura™ are trademarks of Avaya Inc.

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

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

Downloading documents

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

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: Communication Manager changes

This chapter describes the features and enhancements of Release 5.2.1 of Avaya Aura® Communication Manager running on the Avaya S8xxx servers with associated Avaya Media Gateways.

The enhancements for Call Center 5.2.1 are covered in *What's New for Avaya Aura™ Call Center 5.2.1*, 07-602633.

14xx support with firmware download

Support of Avaya 14xx digital telephones

Communication Manager provides support to the Avaya 14xx digital telephones. You can use these telephones on existing systems by translating them or aliasing them to the respective types of Avaya 24xx digital telephones. However, the Avaya 14xx digital telephones will be natively supported later.

The Avaya 14xx digital telephones, namely 1408 and 1416, are firmware downloadable. Firmware download functionality allows you to administer and maintain the Avaya 14xx digital telephones. When you alias or administer the Avaya 14xx digital telephone as the Avaya 24xx digital telephone, Communication Manager allows firmware download to the Avaya 14xx digital telephone (station).

Note:

It is highly recommended that before adding any 14xx station type, you run the **`change alias station`** SAT command to alias the new station types. You can alias the 1408 to a 2410 and the 1416 to a 2420. After aliasing you can run the add, change, remove, or list commands using the respective 14xx station types, which also allows you to easily list all the extensions that you have added with these station types. For example, **`list station type 1408`**.

Requirements for firmware download

Communication Manager supports firmware download to the Avaya 14xx digital telephones if the phone type requesting a download is administered or aliased as the Avaya 2410 or 2420

digital telephone. Communication Manager supports firmware download to the Avaya 1408 and 1416 digital telephones in a similar manner as the Avaya 2410 and 2420 digital telephones. The 1408 and 1416 phone types use the same firmware and it is not the same as those of the 2410 and 2420 phone types.

The following table describes the field values to be added by an administrator for the firmware download:

Screen	Field	Value
Firmware Station-Download	**Download Station Type**	1408/1416
Status Firmware Station Download	**Terminal type for download**	1408/1416
TFTP Server Configuration	**Station Type**	1408/1416

Note:

You can download the firmware of the Avaya 14xx digital telephones by the same methods which are used for the Avaya 24xx digital telephones. The 14xx firmware is about 40% larger than the 24xx firmware so that increases the download time.

Note:

The Avaya 14xx digital telephones are administered as the Avaya 24xx digital telephones in a mixed environment where you have both phone types (14xx and 24xx) within your range of extensions. As these extensions are specified for the scheduled firmware download, you will see “ABORT 8” errors associated with the extensions. For instance, if you have the 14xx firmware loaded in Communication Manager, then the 24xx will reject the firmware while aliasing and Communication Manager will report the “ABORT 8” errors. The errors mention that these extensions are not correct for the current firmware loaded into Communication Manager; however you can ignore the errors.

From Communication Manager 6.0 and later, where the Avaya 14xx digital telephones are natively supported, you can avoid “ABORT 8” errors by correctly administering the extensions as either a 1408 or 1416 phone type.

Comfort noise support

RFC 3389 Comfort Noise

Appears on the Signaling Group screen when the **Group Type** field is sip.

Valid entries	Usage
y	This enables SIP signaling for comfort noise. If **RFC 3389 Comfort Noise** field is set to y, this field overrides the **Silence Suppression** field on the IP Codec Set screen.
n	This disables SIP signaling for comfort noise. Default is n.

Communication Manager upgrades

Most previous releases of Communication Manager can be upgraded to Release 5.2.1. See Supported servers for upgrades (by release) on page 11 for the supported upgrade paths. The upgrade procedures for upgrading to Release 5.2.1 are no different from upgrading to Release 5.2. See *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885 for those procedures.

It is possible to upgrade (migrate) existing Avaya S8xxx servers to the new S8800 and HP DL360 G7 servers. See Supported servers for migrations (Release 5.2.1) on page 13 for the supported migration paths. The Avaya S8800 and HP DL360 G7 servers are used for both simplex and duplex modes. The procedure for upgrading the S8xxx servers to the HP DL360 G7 Server is similar to upgrading the S8xxx servers to the S8800 Server. See the *Upgrading Servers to the Avaya S8800 Server for Avaya Aura™ Communication Manager*, 03-603445 for procedures for upgrading the following servers:

- Avaya S8500-Series Servers to Avaya S8800 Server in simplex mode
- Avaya S8700-Series Servers to Avaya S8800 Server in duplex mode
- Avaya S8500-Series Servers to Avaya S8800 Server in duplex mode

You can also upgrade the simplex S8800 Server to the duplex HP DL360 G7 Server. The procedure for upgrading the simplex S8800 Server to the duplex HP DL360 G7 Server is similar to upgrading the simplex S8800 Server to the duplex S8800 Server.

For the other migration paths, the procedures for upgrading simplex servers to the Avaya S8800 or HP DL360 G7 server and duplex servers to the Avaya S8800 or HP DL360 G7 Server are no different from migrating to the Avaya S8510 or S8730 server, respectively. See *Migrating to Avaya S8xxx Servers and Media Gateways*, 03-300412 for those procedures.

Supported servers for upgrades (by release)

List of servers supported in Release 5.2.1 of Communication Manager:

Servers	Communication Manager										
	1.x	2.0.x	2.1.x	2.2.x	3.0.x	3.1.x	4.0.x	5.0.x	5.1.x	5.2	5.2.1
S8700	✔	✔	✔	✔	✔	✔	✔ *	✘	✘	✘	✘
S8710	✘	✘	✘	✔	✔	✔	✔	✔ +	✔ +	✔ +	✔ +
S8720	✘	✘	✘	✘	✘	✔	✔ ^	✔ ^+	✔ ^+	✔ ^+	✔ ^+
S8730	✘	✘	✘	✘	✘	✘	✘	✔ +	✔ +	✔ +	✔ +
S8500A	✘	✔	✔	✔	✔	✔	✔ *	✘	✘	✘	✘
S8500B	✘	✘	✘	✔	✔	✔	✔ *	✔ *	✔ *	✔ *	✔ *
S8500C	✘	✘	✘	✘	✘	✔	✔	✔	✔	✔	✔
S8510	✘	✘	✘	✘	✘	✘	✘	✘	✔	✔	✔
S8400A	✘	✘	✘	✘	✘	✔	✔	✔	✔ *	✔ *	✔ *
S8400B	✘	✘	✘	✘	✘	✘	✘	✔	✔	✔	✔
S8300A	✔	✔	✘	✘	✘	✘	✘	✘	✘	✘	✘
S8300B	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
S8300C	✘	✘	✘	✘	✘	✘	✔	✔	✔	✔	✔
S8300D	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔
S8100	✔	✔	✘	✘	✘	✘	✘	✘	✘	✘	✘
CSI	✔	✔	✔	✔	✔	✔	✘	✘	✘	✘	✘
SI	✔	✔	✔	✔	✘	✘	✘	✘	✘	✘	✘
R	✔	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘

Note:

* supported with memory upgrade

+ requires DAL2 for hardware duplication

^ XL configuration requires DAL2 with hardware 1 duplication

Legend:

✔ - upgrade path supported, pricing, documentation and translation tool support

✘ - no upgrade path supported (does not preclude circuit pack reuse and manual translation)

Supported servers for migrations (Release 5.2.1)

The supported migration paths for Release 5.2.1 of Communication Manager is contained in the following table:

To → / From ↓	S8300C/D	S8400B	S8510	S8800/HP DL360 G7 Simplex	S8730/S8800/HP DL360 G7		
					Duplex	High	Critical
CSI w/ CMC (note 1)	✘	✔	✔	✔ (note 2)	✔ (note 2)	✔ (note 2,4)	✘
S8100 w/ CMC (note 2)	✘	✔	✔	✔ (note 2)	✔ (note 2)	✘	✘
S8100 w/ G600 (note 1)	✘	✔	✔	✔ (note 2)	✔ (note 2)	✘	✘
SI Simplex	✘	✘	✔ (note 3, 4)	✔ (note 4)	✔ (note 4)	✔ (note 4)	✔ (note 4)
SI Duplex	✘	✘	✘	✘	✔ (note 4)	✔ (note 4)	✔ (note 4)
R Simplex	✘	✘	✘	✔	✔	✔	✔
R Duplex	✘	✘	✘	✘	✔	✔	✔
S8300A/B/C	✔	✘	✘	✘	✘	✘	✘
S8400A	✘	✔	✔	✔ (note 2)	✔ (note 2)	✘	✘
S8400B	✘	✘	✔	✔ (note 2)	✔ (note 2)	✘	✘
S8500A/B/C	✘	✘	✔	✔	✔	✔ (note 4)	✔ (note 4)
S8510	✘	✘	✘	✔	✔	✔ (note 4)	✔ (note 4)
S8700 (IPC/MC)	✘	✘	✘	✘	✔	✔	✔
S8710 (IPC/MC)	✘	✘	✘	✘	✔	✔	✔

To → / From ↓	S8300C/D	S8400B	S8510	S8800/HP DL360 G7 Simplex	S8730/S8800/HP DL360 G7 Duplex	S8730/S8800/HP DL360 G7 High	S8730/S8800/HP DL360 G7 Critical
S8720 (IPC/MC)	✘	✘	✘	✘	✔	✔	✔
S8730 (IPC/MC)	✘	✘	✘	✘	✔ (note 5)	✔ (note 5)	✔ (note 5)
S8800	✘	✘	✘	✔ (note 6)	✔ (note 6)	✔ (note 6)	✔ (note 6)

Note:

1. cabinet does not support duplicate IPSIs
2. merges (system becomes a port network in a larger system) only
3. direct connect only
4. must use G650 (move packs from other cabinet type)
5. S8730 migrates to S8800 or HP DL360 G7
6. S8800 migrates to HP DL360 G7

Legend:

✔ - migration path supported, pricing, documentation and translation tool support

✘ - no migration path supported (does not preclude circuit pack reuse and manual translation)

Kernel Replacement

About kernel replacement

You can replace the Linux kernel using the existing update mechanism in Communication Manager servers including servers that support RAM disk. For procedures on replacing the kernel, see

- Kernel replacement using Communication Manager System Management Interface
- Kernel replacement using Linux commands

Avaya Aura™ SIP Enablement Services (SES) Release 5.2.1 and Avaya Software Update Manager (SUM) also support kernel updates. For more information on replacing the kernel using SUM, see *Avaya Integrated Management Release 5.2 Software Update Manager*.

A kernel update is independent of the following:

- Service pack, security service pack, or SIP Enablement Services updates
- Whether the system is running on the kernel that came with the release or a kernel from a prior update

Note:
Any upgrade to a new load is blocked if a kernel update is in a pending state.

Kernel replacement using System Management Interface

Logging in to System Management Interface (SMI) from your laptop

1. Connect the laptop to the services port (eth1) using a crossover cable.
2. Open Internet Explorer (5.5 or later) on the laptop computer.
3. In the **Address (or Location)** field of your browser, type `192.11.13.6` and press **Enter**.
   If your browser does not have a valid security certificate, you will see a warning screen and instructions to load the security certificate. The system displays the Welcome screen.
4. Click **Continue**.
   The system displays the Logon screen.
5. Log in as `craft`.
6. Select **yes** for `Suppress Alarm Origination`.
   The system displays the main menu for SMI.
7. On the **Administration** menu, click **Server (Maintenance)**.
   The system displays the main menu in the left panel and a usage-agreement notice in the right window.

Downloading the kernel file

Download the latest kernel `.tar` file from the Web site http://support.avaya.com. The kernel file may look like the following: `KERNEL-1.2.34-56.AB04XYZ.tar.gz`.

Note:
A Product Correction Notice (PCN) is issued whenever a new kernel update is available. To view the PCN, visit http://support.avaya.com.

Copying files to the server

1. On the SMI, select **Miscellaneous > Download Files**.
   The system displays the Download Files page.
2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** to open the Choose File window to navigate to the files you want to download.
4. Select the files to download.
5. Click **Download** to copy the files to the server.
   The kernel file is downloaded into the `/var/home/ftp/pub` directory.

   Note:
   To manually FTP files from your laptop to `/var/home/ftp/pub`, you must change the directory to `pub` (type `cd pub`) after starting FTP and logging in.

   The transfer is complete when the system displays the message, `"Files have been successfully downloaded to the server"`.

Installing the kernel update

Important:
Back up the server data before you upgrade the kernel.

1. On the SMI, select **Server Upgrades > Manage Updates**.
   The system displays the Manage Updates page. For more information, see Manage Updates on page 19.
2. If the status of the kernel update file that you want to activate shows `packed` in the `Status` column, select the file (radio button) and click **Unpack**.
   The system displays the status of the unpacking process.
3. After the system displays the message, "`...unpacked successfully`", Click **Continue**.
   The system displays the Manage Updates page.
4. If the update that you want to activate shows `unpacked` in the `Status` column, select the file (radio button) and click **Activate**.
   The system displays the following message on the Manage Updates page.
   `WARNING: Activation of update KERNEL-1.2.34-56.AB04XYZ will cause a server reboot. Do you want to continue?`
5. Click **Yes**.
   The system displays the status of the activation process and will indicate the update was successfully activated. Do not click **Continue** until the automatic reboot has completed. The server reboot takes approximately 3 to 8 minutes. After the server reboots, the new kernel runs.

   Tip:
   When you are waiting for the system to reboot, type `ping -t 192.11.13.6` from a command prompt window on your services laptop computer to start a continuous ping command. If you start getting a reply, the reboot is complete.
6. Verify that your system is running properly. For more information, see Testing the system using the System Management Interface on page 18.
7. Click **Server** > **Process Status**.
   The system displays the default settings for the output of the Process Status report.
8. Click **View**.
   The system displays the process status results.
9. Verify that all processes are active before you return to the Manage Updates page, and click **Continue**.

   Warning:
   You must verify that the server reboot is complete before clicking continue. An automatic server reboot occurs about 1 minute after successful activation of a kernel service pack. You should wait for at least 5 minutes for the server reboot to complete, and for all Communication Manager processes to restart.
10. If the kernel service pack you want to activate shows `Pending_Commit` in the **Status** column, click **File**.

11. Click **Commit**.

    When using Linux commands to activate the kernel service pack, before you commit the service pack, use the **statapp** command after the reboot to verify that all applications are active.

    Perform the steps to commit the kernel service pack for deactivating the kernel service pack. The server reboots after the deactivation. Verify that all processes and applications are active before proceeding.

12. If the update that you want to activate shows `Pending_Commit` in the `Status` column, select the file (radio button) and click **Commit**.

Testing the system using the System Management Interface

1. On the SMI, click **Administration > Server (Maintenance)**.
2. Under **Server** click **Status Summary**. Verify that the `Server Hardware` and the `Processes` fields say `okay`.
3. Under **Diagnostics** select **Ping**.
4. Under **Endpoints to Ping**, select **All IPSI's, UPS's**.
5. Click **Execute Ping**.
   If the ping is successful, the Execute Ping results page displays a brief summary that shows the number of packets sent and received. The summary also shows the minimum, average, and maximum of the round-trip times.
6. From a computer on the customer LAN, use Internet Explorer to connect to the server.
7. Log in as **craft**.
   This action verifies that connectivity exists and the customer can log in to perform administration or other tasks.

Note:

If you do not commit the update within ten minutes of the server reboot, a minor platform alarm is generated. Also, if a reboot occurs before the update is committed, the server will come back up running the original kernel rather than the kernel from the update.

Manage Updates

Use this page to manage the updates. The types of updates are service pack, security service pack, kernel, and SIP Enablement Services updates. This page displays:

- The current release that is running on the server
- Mode of the server
- Updates available for the server and their corresponding status

Manage updates field descriptions

Name	Description
Update ID	The unique update identifier. For example, the Update ID may look like the following for a kernel update: `KERNEL-2.6.18-53.AB04XYZ`.
Status	Displays the status of the current update. • **Activated**: The update is functioning correctly. • **Packed**: A new update is available. • **Unpacked**: A new update is successfully unpacked. • **Pending_Commit**: The kernel update is activated but the activation is not committed. • **Pending_Deactivate**: The kernel update is deactivated but the deactivation is not committed.
Type	Either hot or cold, where cold means the update is service affecting, hot means the update is not service affecting. This page prompts the user to continue if the update is of type cold.
Unpack	Unpacks the update file. The update file is read from the update repository (`/var/home/ftp/pub`).
View	Displays the information about the update file.
Activate	Activates the update file.
Deactivate	Deactivates the update file.
Remove	Removes all the files associated with an update that is not active. If the update is in an *unpacked* state and exists in the update repository, the *update* will show as *packed* after the *unpacked* version is removed.
Commit	Completes the current kernel update process. The system displays the state of the current kernel update. **Note:** The **Commit** button is unavailable if the kernel update is not in the pending state.

Kernel replacement using Linux commands

Connecting a laptop to the server

Prerequisites

Make sure that you have a Secure Shell (SSH) application such as PuTTY installed on your laptop.

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the Host Name (or IP Address) field, type **192.11.13.6**.
4. In the Protocol area, click **SSH**.
5. In the Port field, type **10022**.
6. Click **Open**.

   Note:

   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the server's host key and display the PuTTY window.
8. Log on as **craft** or **dadmin**.
9. Type **Exit** and press **Enter** to close PuTTY.

Downloading the kernel file

For instructions to download the kernel file, see Downloading the kernel file on page 16.

Copying files to the server

For instructions to copy the kernel file, see Copying files to the server on page 16.

Installing the kernel file

Important:
Back up the server data before you upgrade the kernel.

1. Type `update_unpack` and press **Enter**.
2. Select the file that corresponds to the kernel file and press **`Enter`**.
3. Type `update_show` and press **Enter** to verify if the new kernel file is unpacked.
4. Type `update_activate` *kernel_name* where *kernel_name* is the release or the issue number of the latest kernel file.

   Note:
   Do not use the `.tar.gz` extension at the end of the file name.
5. Press **Enter**. The system displays the following message, `"WARNING: Activating this update will cause a server reboot. Continue?"`
6. Type `y` and press **Enter**.
   The server reboot takes approximately 3 to 8 minutes. After the server reboots, the new kernel runs.

   Tip:
   When you are waiting for the system to reboot, enter `ping -t 192.11.13.6` from a command prompt window on your services laptop computer to start a continuous ping command. If you start getting a reply, the restart is complete.
7. Log on to the server from a Services laptop computer with an SSH client. For more information, see Connecting a laptop to the server on page 20.
8. Verify that your system is running properly. For more information, see Testing the system using the System Management Interface on page 18.
9. Type `update_show` and press **Enter** to verify if the status of the kernel file is `pending_commit`.
10. Type `statapp` and press **Enter** to verify all processes are active before committing the kernel service packs.
11. Type `update_commit` and press **Enter**.

    Note:
    If you do not run the **`update_commit`** command within ten minutes of the server reboot, a minor platform alarm is generated. Also, if a reboot occurs before the

update is committed the server will come back up running the original kernel rather than the kernel from the update.

12. Type `update_show` and press **Enter** to verify if the status of kernel file is `Activated`.

Modifications to the existing commands

update_show

Syntax

```
update_show [-a] [-c] [-h] [-k] [-u]
```

-a Display the activated updates only.

-c Display the updates in a pending state and the number of kernel updates.

-h Display the command option descriptions.

-k Display the details of the kernel updates.

-u Display the unpacked updates only.

Description

Use **update_show** to display the information about a specified software or kernel update.

update_activate

Syntax

```
update_activate [-h]
```

-h Display the help information.

Description

Use **update_activate** to activate a previously unpacked update on the server. Updates cannot be activated when a kernel update is in a pending state.

update_deactivate

Syntax

```
update_deactivate [-h]
```

-h Display the help information.

Description

Use **update_deactivate** to deactivate a previously activated update on the server. Updates cannot be deactivated when a kernel update is in a pending state.

No-cadence call classification modes and End OCM timer

Detailed description of No-cadence call classification modes and End OCM timer

Use the No-cadence call classification modes and End OCM timer feature to improve the call classification time and accuracy used for voice and answering machine call classification.

This feature provides two classifier modes:

- ISDN answered call with AMD on mode – Detects live voice with answering machine detection (AMD).
- ISDN answered call with AMD off mode – Detects live voice without AMD.

These two modes do not detect any call progress tone cadence except Special Information Tone (SIT) and MODEM/FAX Answer Back tone.

This feature also provides an administrable timer (End OCM timer) to ensure that an outgoing call using OCM call classification is answered by an agent or an announcement within a specified time. The timer is turned off if the call drops or terminates to a port. If the timer expires, Communication Manager disconnects the call classifier and connects the call to an announcement.

Communication Manager is administrable per system to put the classifier into one of the two modes depending on whether it receives a connect or answer supervision message from an outbound trunk.

Note:

The classifier modes without call progress cadence detection do not need to be used with the End OCM timer and the reverse is also true. The classifier modes with call progress detection can be used with the End OCM timer.

Communication Manager administers per system whether classifiers use the new classification modes. If you upgrade the Communication Manager software, by default the classifier uses the old modes. If you do a new installation of the Communication Manager software, by default the classifier uses the no-cadence call classification modes.

Communication Manager administers per location the maximum amount of time after answer that classifiers can spend trying to classify each OCM call. The timer ranges from 100 to 25,000 milliseconds in increments of 100 milliseconds. It defaults to blank, which means no limit.

Communication Manager administers per location an extension number to route the call when the maximum classification time is reached. The number can be a recorded announcement, a vector directory number, a hunt group extension, or blank. The **End of OCM intercept Extension** field cannot be left blank if the **End OCM After Answer** timer field contains a non-blank value.

Firmware requirements for No-cadence call classification modes and End OCM timer

For the TN744FP, TN2312AP/BP, and TN8412AP circuit packs, the respective firmware vintages 3, 48, and 18 or greater are required to support this feature.

For the G250, G350, G430, G450, and G700 media gateways, firmware version load 30.10.x or greater is required to support this feature.

Call processing scenarios

The following is a list of call processing scenarios for the No-cadence call classification modes and End OCM timer feature:

ISDN trunk

When connecting a classifier to a call, Communication Manager instructs the classifier to use the no-cadence call classification modes if the following conditions are satisfied:

- The call is an OCM switch-classified call over an ISDN trunk.
- Older releases of Communication Manager use the corresponding older AMD on or AMD off modes.
- The **Cadence Classification After Answer** field on the **System Parameters OCM Call Classification** screen is set to N.
- Communication Manager has received a connect message from the far end of the trunk, and satisfies one of the following:
  - The **CONNECT Reliable When Call Leaves ISDN** field on the **ISDN Trunk Group** screen is set to Y.
  - The **CONNECT Reliable When Call Leaves ISDN** field on the **ISDN Trunk Group** screen is set to N but Communication Manager has not yet received a Progress Indication message that the call is not end-to-end ISDN or the call has a non-ISDN destination address.

SIP trunk

When connecting a classifier to a call, Communication Manager instructs the classifier to use the no-cadence call classification modes if the following conditions are satisfied:

- The call is an OCM switch-classified call over a SIP trunk.
- Older releases of Communication Manager use the corresponding older AMD on or AMD off modes.
- The **Cadence Classification After Answer** field on the **System Parameters OCM Call Classification** screen is set to N.
- Communication Manager has received an answer signal from the far end of the trunk.

Other trunks (Non-ISDN & Non-SIP)

When connecting a classifier to a call, Communication Manager instructs the classifier to use the no-cadence call classification modes if the following conditions are satisfied:

- The call is an OCM switch-classified call over a non-ISDN or a non-SIP trunk.
- Older releases of Communication Manager use the corresponding older AMD on or AMD off modes.
- The **Cadence Classification After Answer** field on the **System Parameters OCM Call Classification** screen is set to N.
- The **Answer Supervision Timeout** field on the **Trunk Group** screen is set to 0.
- The **Receive Answer Supervision** field on the **Trunk Group** screen is set to y.
- Communication Manager has received an answer signal from the far end of the trunk.

Mixture of old and new classifiers

If an IP-connected media gateway or port network has a mixture of new classifiers that understand the no-cadence call classification modes and old classifiers that do not understand the no-cadence call classification modes, call processing tries to use the new classifiers for OCM calls. If all new classifiers are busy, call processing uses the old classifiers for OCM calls.

End OCM timer

- If the **End OCM After Answer** timer field is set to a non-blank value, Communication Manager starts the timer for OCM calls after receiving a Connect message or an answer supervision signal from the network.
- When the End OCM timer expires, Communication Manager connects the originating end of the call to the extension administered in the **End of OCM Intercept Extension** field on the **Location Parameters** screen.

Active VDN

If CTI application requests a third party make call with an originating VDN, Communication Manager sets the originating VDN as the active VDN. When the End OCM timer expires, Communication Manager re-routes the call to End of OCM Intercept Extension. If the **Allow VDN Override** field is set to `n`, the End of OCM Intercept Extension starts processing the call but internal to Communication Manager the active VDN is still remembered as the originating VDN.

Administering No-cadence call classification modes and End OCM timer

The following steps are part of the administration process for the No-cadence call classification modes and End OCM timer feature:

- Setting up no-cadence call classification modes
- Setting up End OCM timer and announcement extension

This section describes:

- The screens that you use to administer the No-cadence call classification modes and End OCM timer feature
- Complete administration procedures for the No-cadence call classification modes and End OCM timer feature

Related topics:

Setting up no-cadence call classification modes on page 26
Setting up End OCM timer and announcement extension on page 27

Screens for administering No-cadence call classification modes and End OCM timer

Screen name	Purpose	Fields
System Parameters OCM Call Classification	Set up the no-cadence call classification modes.	**Cadence Classification After Answer**
Location Parameters	Set up the time interval in milliseconds, for the End OCM timer.	**End OCM After Answer (msec)**
	Set up the announcement extension.	**End of OCM Intercept Extension**

Setting up no-cadence call classification modes

1. Type **change system-parameters ocm-call-classification**. Press Enter. The system displays the System Parameters OCM Call Classification screen.
2. Set the **Cadence Classification After Answer** field to n.
3. Press Enter to save your changes.

Setting up End OCM timer and announcement extension

1. Type **change location-parameters**. Press Enter. The system displays the System Parameters OCM Call Classification screen.
2. In the **End OCM After Answer (msec)** field, type the desired timeout value in milliseconds. Valid entries are a number from 100 to 25,000, or blank. In the **End of OCM Intercept Extension** field, type the extension number that you want to assign. The number can be a recorded announcement, a vector directory number, or a hunt group extension.
3. Press Enter to save your changes.

Considerations for No-cadence call classification modes and End OCM timer

This section provides information about how the No-cadence call classification modes and End OCM timer feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of no-cadence call classification modes and End OCM timer under all conditions. The following considerations apply to the No-cadence call classification modes and End OCM timer feature.

Announcements

To prevent delays while connecting the announcement,

- You can configure Communication Manager with a large pool of announcement boards.
- You can configure Communication Manager to use integrated-repeating announcements. That announcement type lets calls use the announcement port even if it is already in use.

For either of these configurations each gateway with public network trunks must have its own announcement port(s) local to the gateway for use by the Locally Sourced Announcements feature.

Performance impact

The values of the **AMD Treatment Talk Duration** and **AMD Treatment Pause Duration** fields on the **SIT Treatment for Call Classification** screen can affect the classification time. This feature decreases call classifier holding times, but increases recorded announcement usage.

Call Management System (CMS) and Avaya IQ

You can administer CMS to provide a report of the percentage of calls that were answered by a live person but timed out before an agent could be connected and were instead connected to the **End of OCM Intercept Extension**.

AMD false positives

You can administer call classification timers to maintain a low rate of false positive answering machine detections, disregarding other outside influences. However, a certain false positive answering machine detection rate is expected because of factors such as the variability in how people answer the telephone with different greetings.

AMD for non-AMD call center

Call center can allow in its calculations to ignore the calls that were answered on the far end by answering machines. You can administer a non-AMD call center to route live voice calls other than the answer machine calls to prove that less than the allowable percentage of live voice calls were abandoned for lack of an agent.

Ringing regulation

Call center can allow outbound calls to ring for certain amount of seconds (the ringing regulation varies from country to country), if the calls are not answered by the called party. You can satisfy the regulation by doing the following:

- Program the CTI application to use third party make call option and **max_ring_cycles** fields.
- Instruct call center agents to not drop calls until the specific number of seconds after being connected to a ringing call.

Tenant

The No-cadence call classification modes and End OCM timer feature can be used with a single Communication Manager server being shared among multiple tenants, each of which has its own announcement. To support multiple tenants the CTI adjunct needs to predetermine the originating VDN to use with third party make call, at least one originating VDN per tenant. You can administer the End of OCM Intercept Extension field with a single VDN which in turn route the call to the correct announcement for each tenant.

Alternatively, you can use a single originating VDN extension shared among multiple tenants, and send the call back into CTI handling through an adjunct routing step. The CTI application can direct the call to an announcement corresponding to the calling tenant. This alternative strategy takes more time compared to the VDN strategy.

Interactions for No-cadence call classification modes and End OCM timer

This section provides information about how the No-cadence call classification modes and End OCM timer feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of the No-cadence call classification modes and End OCM timer feature in any feature configuration.

Multi-National/Global Considerations

The **Cadence Classification After Answer** field on the **System Parameters OCM Call Classification** screen is administered per system rather than per location.

The **End OCM After Answer** timer field is administered per location. Different countries are likely to have different timing regulations.

The **End of OCM Intercept Extension** field is administered per location. Different countries are likely to have announcements in different languages.

TTY classification

The call classifier currently does not have TTY detection. You can record an announcement both in the local language and in TTY. The **End of OCM Intercept Extension** field can contain an announcement recorded both in the local language(s) and in TTY.

Call classification after answer supervision

The call classification after answer supervision feature is independent of the no-cadence call classification modes and End OCM timer feature.

CONNECT reliable when call leaves ISDN

The No-cadence call classification modes and End OCM timer feature is dependent on the **CONNECT reliable when call leaves ISDN** field.

Answer supervision timeout

If answer supervision is enabled, set the **Answer Supervision Timeout** field to 0 (zero).

Private network ISDN (QSIG)

Communication Manager sends an update message to the QSIG trunk when the following happens:

- The outgoing trunk uses private network QSIG signaling.
- Communication Manager changes the originator from the one specified by the CTI adjunct's third party make call request to the End of OCM Intercept Extension.

It is the same message used if a person manually transfers a call. However, a call center is unlikely to make outgoing calls over QSIG trunks.

SIP

Communication Manager sends an update message to the SIP trunk when the following happens:

- The outgoing trunk uses SIP signaling.
- Communication Manager changes the originator from the one specified by the CTI adjunct's third party make call request to the End of OCM Intercept Extension.

CCRON

Communication Manager does not share the no-cadence call classification modes with the Coverage of Calls Redirected Off-Net (CCRON) capability.

EC500

Communication Manager does not share the no-cadence call classification modes with the Extension to Cellular (EC500) capability.

Call vectoring

Call vectoring works with the No-cadence call classification modes and End OCM timer feature.

Inter-Gateway Alternate Routing

If you have a single PBX for both call center and non-call center communication, a call center with strict timing regulations can use Inter-Gateway Alternate Routing (IGAR). You must make sure that each gateway with public network trunks has its own announcement port(s) for use by the Locally Sourced Announcements feature. This helps prevent delays while connecting the announcement.

Call Redirection

Communication Manager 5.2.1 treats an OCM call the same way as the Communication Manager 5.0 third party make call feature, when the following happens:

- Communication Manager terminates an OCM call to the End of OCM Intercept Extension.
- End of OCM Intercept Extension is administered as a VDN.
- Associated vector has a route-to step.

The call proceeds to the route-to destination. If the call terminates at a busy endpoint, Communication Manager drops the call.

Uniform Dial Plan

Communication Manager administers per location an extension number to route the call when the maximum classification time is reached. The extension number can be a recorded announcement, a vector directory number, or a hunt group extension on the local server. The field does not accept a UDP extension, even if the extension routes to a recorded announcement on another server.

Multi-location ARS routing

The location of the outgoing trunk is used for the OCM call when the following happens:

- Communication Manager terminates an OCM call to the End of OCM Intercept Extension.
- **End of OCM Intercept Extension** is administered as a VDN.
- Associated vector has a route-to step.

Multi-Location Dial Plan (MLDP)

The Multi-Location Dial Plan feature analyses digit strings via entries in the UDP tables. The **End of OCM Intercept Extension** cannot be administered as a UDP extension. You can type the full extension number into the administration field.

Location Parameters

End OCM After Answer (msec)

If the **End OCM After Answer** field contains a non-blank value, Communication Manager starts the End OCM timer when Communication Manager receives an answer signal. The End OCM timer ensures that an outgoing call using OCM call classification is answered by an agent or an announcement within a specified time.

Valid Entry	Usage
100 to 25,000	The timeout value is in milliseconds. If the timer expires, Communication Manager disconnects the call classifier and connects the call to the administered intercept extension. If the call classifier classifies the call before the timer expires, the timer is cancelled and the call routed or treated appropriately.
blank	Indicates that the timer has no limit.

End of OCM Intercept Extension

Valid Entry	Usage
extension	The extension number Communication Manager connects the call to when the **End OCM After Answer** field expires. The extension number can be a recorded announcement, a vector directory number, or a hunt group extension.
blank	Indicates that the extension number is empty. If the **End OCM After Answer** field is set to a non-blank value, the **End of OCM Intercept Extension** field cannot be left blank.

System Parameters OCM Call Classification

Cadence Classification After Answer

Valid Entry	Usage
y	Old classifier detects live voice with or without AMD. These modes detect call progress tone cadence. If you upgrade the Communication Manager software, by default the classifier uses the old modes. If you do a new installation of the Communication Manager software, by default the classifier uses the no-cadence call classification modes.
n	No-cadence call classification modes detect live voice with or without AMD whenever Communication Manager receives a connect or answer supervision message from an outbound trunk. These modes do not detect any call progress tone cadence.

Connection Manager Denial events

DNY_CLASS_NO_CAP

Table 1: Connection Manager denial events

Event Type	Event Description, as it appears on the event log	Explanation	Event Data 1	Event Data 2
2399	DNY_CLASS_NO_CAP	CPTR with no-cadence capability requested, not found.		

Special application activation process

Special applications, also known as green features, meet special requirements requested by one or more customer. Until now, Avaya has charged a fee to the customer to activate the special application. Communication Manager now offers many of these special applications to all customers at no additional cost and no change to the license. Customers may activate the special applications by themselves using their own super-user login. Although these special features are available to customers, they may have not gone through extensive testing. So customers must use at their own risk.

Some of the special features should not be set without the right configurations, and some features should not be set together at the same time. Otherwise, the feature may not operate as expected, the system performance could be affected or both. To avoid users from setting those features accidentally, Communication Manager has identified those features and marked them as restricted. For those restricted features, customers must contact Avaya's Custom Development team to activate.

For a list of these unrestricted special features and information about them, see *Avaya Aura™ Communication Manager Special Application Features*, which is available on http://support.avaya.com.

Connection-preserving updates for duplicated servers

You can apply connection-preserving updates to the S87xx and the Avaya S8800 duplicated servers running current version of Communication Manager, while phone calls continue without interruption. However, the following connections are not preserved during a connection-preserving update:

- H.323 IP trunks
- SIP trunks (for example, trunks established for SIP endpoints that use Communication Manager and SES for SIP connections)
- ISDN-BRI trunks or stations
- Some ISDN-PRI trunks
- Unstable calls (for example, the calls that are in the ringing or dialing state, calls on hold, and calls in any state that require control signaling)
- SAT sessions
- Adjunct links (for example, links to CMS, ASAI, CDR, system printers, and links configured using the IP Services screen)
- All connections in a server hardware migration

Note:

During the update process, Communication Manager does not allow the use of additional calling features on preserved connections.

The System Management Interface (SMI) is enhanced to enable application of connection-preserving updates. During the Pre Update/Upgrade process, data is synchronized between active and standby servers, maintaining the state of service during the interchange of active and standby servers. The interchange occurs on demand or when the health of the active server fails. After the update process is complete, all IP telephones re-register with the Communication Manager. However, an IP telephone whose call is preserved during the update process, re-registers with the Communication Manager only after the call is complete.

Workflow for applying connection-preserving updates

#	Task	Instructions
1	On the active and standby servers, save translations.	1. Start an SSH session and access 192.11.13.6 5022. 2. At the login prompt, type `dadmin`. 3. At the password prompt, enter the password for the dadmin login ID and press **Enter**. 4. On the SAT interface prompt, type `save translations` and press **Enter**.
2	On the active and standby servers, back up data.	1. Log on to the SMI. 2. Click **Administration** > **Server (Maintenance)**. 3. Select **Data Backup/Restore** > **Backup Now**. 4. Select **Full Backup**. 5. Click **Start Backup**.
3	On the active and standby servers, download the software update and copy the software update to the server.	Download the update file from the Web site http://support.avaya.com. For information about copying files to the server, see Copying files to the server on page 16.
4	On the active server, complete the Pre Update/Upgrade Step tasks.	1. Select **Server Upgrades** > **Pre Update/Upgrade Step**. 2. Click **Continue**.
5	On the standby server, activate the update.	1. Select **Server Upgrades** > **Manage Updates**. 2. If the status of the update file that you want to activate shows `packed` in the `Status` column: a. Select the update file (radio button). b. Click **Unpack**. c. After the system displays the message, "`...unpacked`

#	Task	Instructions
		successfully", click **Continue**. 3. If the status of the update file that you want to activate shows `unpacked` in the `Status` column: a. Select the file (radio button). b. Click **Activate**. The system displays the status of the activation process.
6	On the standby server, verify the status.	1. Select **Server** > **Status Summary**. 2. Look up the `Standby Refreshed?` value.
7	On the standby server, activate a server interchange.	Do one of the following: If the `Standby Refreshed?` value is `yes (for update/upgrade)`: a. Select **Server** > **Interchange Servers**. b. Click **Interchange**. If the `Standby Refreshed?` value is `no`: a. Select **Server** > **Interchange Servers**. b. Select the **Force interchange regardless of server status** check box. **Important:** Selecting **Force interchange regardless of server status** results in a cold interchange and connections are not preserved. c. Click **Interchange**.
8	On the new standby server, activate the update.	On the new standby server, perform the instructions listed in task 5.
9	On the new standby server, verify the status.	On the new standby server, perform the instructions listed in task 6.

For more information on applying connection-preserving updates, see the System Management Interface (SMI) help.

Communication Manager Feature Server configuration

Communication Manager is configured as a feature server by administration options of the SIP interfaces on Communication Manager. Any server which supports Communication Manager also supports the feature server configuration.

Communication Manager configured as a feature server does not support non-SIP stations, but does support non-SIP trunking. For more information on how to configure Communication Manager as a feature server, see *Administering Avaya Aura® Communication Manager as a Feature Server, 03–603479* for Release 5.2.

Chapter 2: Avaya Media Gateways changes

This chapter summarizes the changes in functionality in Media Gateways for Communication Manager 5.2.1

G450 - increased capacity

The G450 now supports a total of 320 VoIP channels.

Note:
The increased capacity is only available when the G450 has registered with a server running Communication Manager 5.2.1 or later.

The output of the **`show voip-parameters`** CLI command reflects the new value:

show voip-parameters

Syntax

```
show voip-parameters
```

Description

Use the **`show voip-parameters`** command to display information about the VoIP engine.

User Level

read-only

Context

general

Example

To display VoIP information:

```
G450-001(super)# show voip-parameters
VOIP ENGINE PARAMETERS
------------------------------------------------------------
IP (PMI)            : 149.49.71.15
Fault Status        : No Fault Messages
Additional Status   : No Status Messages

CURRENT STATE
------------------------------------------------------------
```

```
In Use     : 0 of 320 channels, 0 of 9600 points (0.0% used)
...
```

MP20 - increased capacity

The G430 and G450 now support 25 VoIP channels on the MP20 Media Processor module.

Note:
The increased capacity is only available when the G430 or G450 has registered with a server running Communication Manager 5.2.1 or later.

The outputs of the following CLI commands reflect the new value:

- **show voip-parameters**
- **show voip-dsp**
- **show system**
- **show platform mainboard**

Avaya G430 CLI commands

show voip-dsp

Syntax

```
show voip-dsp [dsp-id]
```

dsp-id Keyword indicating the slot number of the VoIP DSP childboard.

dsp-id Possible values:

- 1 - onboard DSP
- 2 - replaceable DSP

Description

Use the **show voip-dsp** command to display information about the DSP and DSP cores parameters, status and occupancy.

User Level

read-only

Context

general

Example

To display DSP parameters use:

```
G430-???(super)# show voip-dsp

DSP #1 PARAMETERS
----------------------------------------------------------------
Board type     : 25 Channels on board VoIP DSP
Fw Vintage     : 16

DSP#1 CURRENT STATE
----------------------------------------------------------------
In Use         : 0 of 25 channels, 0 of 750 points (0.0% used)
State          : Idle
Admin State    : Release
```

show voip-parameters

Syntax

```
show voip-parameters
```

Description

Use the **show voip-parameters** command to display information about the VoIP engine.

User Level

read-only

Context

general

Example

To display VoIP information:

```
G430-003(super)# show voip-parameters

VOIP ENGINE PARAMETERS
----------------------------------------------------------
IP (PMI)            : 149.49.71.15
Fault Status        : No Fault Messages
Additional Status   : No Status Messages

CURRENT STATE
----------------------------------------------------------
In Use     : 0 of 105 channels, 0 of 3150 points (0.0% used)

VoIP-DSPs PARAMETERS
----------------------------------------------------------
VoIP Child Type SUFFIX HW      FW      Chan  Admin   Oper    Fault
Slot Board             VINTAGE VINTAGE InUse State   State   Status
---- ----- ---- ------ ------- ------- ----- ------- ------- ---------
1    On board(25)      N/A     16       0/25 Release Idle    No Error
```

```
2    VOIP  MP80 B      0       16       0/80 Release Idle    No Error
...
```

Note:

If the G430 is registered to versions of Communication Manager prior to 5.2.1 that do not support the increased capacity, you see the following message:

```
Note: The gateway is registered with a Communication Manager version which limits
DSP resources to 100 channels.
```

show system

Syntax

```
show system
```

Description

Use the **show system** command to display information about the device.

User Level

read-only

Context

general

Example

To display device information:

```
G430-???(super)# show system
System Name                 :
System Location             :
System Contact              :
Uptime (d,h:m:s)            : 2,18:20:56
MV Time                     : 09:39:53 26 MAR 2009
Serial No                   : 08IS26191007
Model No                    : G430
HW Ready for FIPS           : No
HW Vintage                  : 4
HW Suffix                   : F
FW Vintage                  : 29.22.1
LAN MAC Address             : 00:07:3b:e4:67:b9
SERVICES MAC address        : 00:07:3b:e4:67:b8
RAM Memory                  : 512MB
Compact Flash Memory        : CompactFlash card is disabled
Main PSU                    : 175W
Media Socket #1             : 25 channels on board VoIP DSP
Media Socket #2             : MP20 VoIP DSP Module
FANS                        : No Fault messages
Expansion module #1         : OK
Expansion module #1 PSU     : 175W
Expansion module #1 POE PSU : Not present
Expansion module #1 FANS    : No Fault messages
Expansion module #2         : Not Present
```

show platform mainboard

Syntax

```
show platform mainboard
```

Description

Use the **show platform mainboard** command to display the main board parameters and the list of media gateway equipment installed in the sockets on the main board.

User Level

admin

Context

general

Example

To display the main board parameters and the media gateway equipment list:

```
G430-???(super)# show platform mainboard
MAINBOARD BOARD
------------------
Type                      : G430
Description               : Avaya Inc., G430 Media Gateway
Serial Number             : 08IS26191007
HW Vintage                : 4
HW Suffix                 : F
FW Version                : 29.22.1
Faults                    : No Fault Messages

RAM MEMORY SOCKET #1
------------------
Type                      : 512MB DDR SDRAM memory module
Serial Number             : 0b2c7605
Manufacture Part Num      : 64A6M64M8L-A06EWQU
Faults                    : No Fault Messages

COMPACT FLASH MEMORY
--------------------
Type                      : CompactFlash card is disabled
Serial Number             : N/A
Model Number              : N/A
Faults                    : N/A

MEDIA SOCKET #1
--------------------
Type                      : 25 channels on board VoIP DSP
Description               : VoIP DSP resource with 20 channels
Faults                    : No Fault Messages

MEDIA SOCKET #2
--------------------
Type                      : MP20 VoIP DSP Module
Description               : VoIP DSP resource with 25 channels
Serial Number             : 08IS18183392
HW Vintage                : 1
HW Suffix                 : A
Faults                    : No Fault Messages
```

Avaya G450 CLI commands

show voip-dsp

Syntax

```
show voip-dsp [dsp-id]
```

dsp-id Keyword indicating the slot number of the VoIP DSP childboard.

dsp-id Possible values: 1 to 4

Description

Use the **show voip-dsp** command to display information about the DSP and DSP cores parameters, status and occupancy.

User Level

read-only

Context

general

Example

To display DSP parameters use:

```
G450-003(super)# show voip-dsp
DSP #1 PARAMETERS
-----------------------------------------------------------------
Board type     : MP20
Hw Vintage     : 2 A
Fw Vintage     : 16

DSP#1 CURRENT STATE
-----------------------------------------------------------------
In Use         : 0 of 25 channels, 0 of 750 points (0.0% used)
State          : Idle
Admin State    : Release

Core# Channels Admin     State
      In Use   State
----- -------- --------- -------
    1  0 of 25  Release Idle
....
```

show voip-parameters

Syntax

```
show voip-parameters
```

Description

Use the **show voip-parameters** command to display information about the VoIP engine.

User Level

read-only

Context

general

Example

To display VoIP information:

```
G450-001(super)# show voip-parameters

VOIP ENGINE PARAMETERS
------------------------------------------------------------
IP (PMI)             : 149.49.70.159
Fault Status         : No Fault Messages
Additional Status    : No Status Messages

CURRENT STATE
------------------------------------------------------------
In Use     : 0 of 25 channels, 0 of 750 points (0.0% used)

VoIP-DSPs PARAMETERS
------------------------------------------------------------
VoIP Child Type SUFFIX HW      FW      Chan  Admin   Oper    Fault
Slot Board             VINTAGE VINTAGE InUse State   State   Status
---- ----- ---- ------ ------- ------- ----- ------- ------- ---------
1    VOIP  MP20 A      2       16       0/25 Release Idle    No Error
2    -- Not Installed --
3    -- Not Installed --
4    -- Not Installed --
Done!
```

Note:

If the G450 is registered to versions of Communication Manager prior to 5.2.1 that do not support the increased capacity, you see the following message:

```
Note: The gateway is registered with a Communication Manager version which limits
DSP resources to 240 channels.
```

ARP spoofing protection

ARP spoofing protection prevents attackers from exploiting gratuitous ARPs to create DoS (Denial of Service) or “man-in-the-middle” attacks.

ARP spoofing protection works by only learning new ARP entries from Unicast ARP replies that were sent as response to gateway ARP requests packets.

Note:
ARP Spoofing protection is not supported on the Services port.

The user activates or deactivates the ARP spoofing protection using the ip arp inspection CLI command:

ip arp inspection

Syntax

```
[no] ip arp inspection
```

Description

Use the **ip arp inspection** command to enable or disable ARP spoofing protection.

User Level

admin

Context

general

Example

To enable ARP spoofing protection:

```
G430-001(super)# ip arp inspection
```

To disable ARP spoofing protection:

```
G430-001(super)# no ip arp inspection
```

Logging enhancements

The media gateways comply with Avaya’s new standard common log format. The format is

```
< PRI > Date stamp hostname MSG
```

PRI

This is defined by RFC 3164. It represents the facility and severity of the message.

Header

The header part contains a timestamp and an indication of the hostname or IP address of the device.

MSG

The gateways will support the additional fields as part of the MSG section in the syslog and log entries presented in CLI session, view of log file and the log-file uploaded to remote server. See the Additional Fields for MSG table.

Table 2: Additional Fields for MSG

Sl no	Item	Common Logging Format SRAD Description	Gateway Field Value
1	TAG [Process ID]	TAG is the name of the application.	The gateway will present "-NoTAG:".
2	UTC Offset	UTC offset.	The gateway will present only "-NoUTC"
3	Year	4-digit year - If not supported or unknown then 0000.	The gateways will present the year based on MV time if the gateway is registered; RTC time if it is not (G430, G450 and new G250/G350 C/S:4.0/3.1 respectively and above).
4	Milliseconds	Milliseconds in 3-digit format.	milliseconds
5	Log format	Value "1" presents the current log format header defined	The gateway will present "1"
6	Product Type	The product type name:	The gateways will present: ".mediagateway.g450", ".mediagateway.g430", ".mediagateway.g350", ".mediagateway.g250", ".mediagateway.g250bri", ".mediagateway.g250ds1", ".mediagateway.g250dcp"
7	Marker	The "|" character indicates the start of the message.	The gateway will present "|"
8	Message format	Value 0 for representation of non- events logs. Value 1 and 2 for events logs.	The gateway will support only value "0" for non-events logs.

Sl no	Item	Common Logging Format SRAD Description	Gateway Field Value
9	Mnemonic	A 32-byte string that briefly describes the log message.	
10	Marker	The "[" character separates between the mnemonic and syslog filtering group/ severity.	The gateway will present "["
11	Syslog filtering group	The user selects the group using the CLI.	
12	Syslog severity	The user selects the severity using the CLI.	

Example

Examples of the new syslog/log:

```
<190>Apr 21 16:28:32 149.49.77.11 -NoTag: -NoUTC 2009 055 1 mediagateway.g430 | 0
coldStart[BOOT-Informational: System boot up from cold reset, ID=N/A
<187>Apr 21 16:28:32 149.49.77.11 -NoTag: -NoUTC 2009 525 1 mediagateway.g430 | 0
MSY-TRPMAJNA[VOICE-Error: No Call Controller Found, ID=N/A
<190>Apr 21 14:30:25 149.49.77.11 -NoTag: -NoUTC 2009 965 1 mediagateway.g430 | 0
BOOT MESSAGE[BOOT-Informational: Booting from bank B with firmware version
29.22.50, ID=N/A
<190>Apr 21 14:30:25 149.49.77.11 -NoTag: -NoUTC 2009 965 1 mediagateway.g430 | 0
coldStart[BOOT-Informational: System boot up from cold reset, ID=N/A
<187>Apr 21 14:30:25 149.49.77.11 -NoTag: -NoUTC 2009 425 1 mediagateway.g430 | 0
MSY-TRPMAJNA[VOICE-Error: No Call Controller Found, ID=N/A
```

power-down reset

Technicians can use this command to power cycle G450 main board. The command is useful if there is some hardware malfunction in one of the components and a soft or hard reset cannot restore functionality.

This command is the same as disconnecting the G450 from the main power supply and reconnecting it or removing the G450 main board and reinserting it.

Note:

This command applies to the G450 main board only; however, there may be disruption to S8300 connectivity during the G450 boot process.

reset power-down

Syntax

```
reset power-down
```

Description

Use the reset power-down command to perform a power cycle on the G450.

User Level

admin

Context

general

Example

To perform a power down reset:

```
G450-001(super)# reset power-down
```

Note:

This command is available on the G450 2.x or later only.

- On the G450 version 1.x, the ASB button is to the right of the RST button.
- On the G450 version 2.x, the ASB button is above the RST button.

Note:

This command is service-disrupting.

Chapter 3: Communication Manager Messaging changes

Install Avaya Aura® Communication Manager Messaging on S8800 and HP DL360 G7 servers

New server support for Communication Manager Messaging

Configure an S8800 or a HP DL360 G7 Server in simplex mode to install Communication Manager Messaging. Installing Communication Manager on page 61.

Note:

Communication Manager Messaging can only be configured on a main server. An S8800 or a HP DL360 G7 Server with Communication Manager Messaging installed does not support configuration on an LSP or an ESS server.

For all other tasks related to installing Communication Manager Messaging on an S8800 or a HP DL360 G7 Server, refer to *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration* 03-603353.

Installing Communication Manager Messaging

For instructions to install Communication Manager Messaging, see Installing Communication Manager on page 61.

Secure Real-Time Transport Protocol

Overview

SRTP protocol seamlessly encrypts audio streams for calls over Communication Manager Messaging. It allows AES-128-CM encryption with 32 and 80-byte authentication.

Note:
TN2302 media processors do not support SRTP.

Logging in to the Communication Manager server using PuTTY

Prerequisites

PuTTY application

1. Open a PuTTY window.
2. In the **Host Name (or IP address)** field, enter the IP address of the Communication Manager server.
3. Select **SSH**.
4. Click **Open**.

Accessing the Communication Manager Server

1. On the SSH screen, type the user credential for the `init` user.
2. Press `Enter` for the terminal type.
3. Press `y` or n to set the session priority.
4. Type `sat`.

5. Provide the password for the init user type.
6. Type `w2ktt` on the terminal type prompt.

Changing customer options to enable media encryption

1. Log in to Communication Manager server using putty.
2. On the SAT screen, type `change system-parameters customer`.
3. On page 4, set the **enable-Media Encryption** field to `y`.
4. Type `save trans`.
5. Press `Esc+X` to exit.

Changing signaling group to enable media encryption

1. On the SAT screen, type `change signaling-group` *x*, *x* is the signaling group number.
2. Ensure the **media encryption** field is set to `y`.
3. Set the password in the **passphrase** field.

Note:
Password can range from 8 through 30 characters. It can contain alphabets, numeric symbol, and letters, and numerals.

Important:
Remember the password you set in the **passphrase** field. For SRTP to function, provide the password in Switch Link Admin Web page on the Messaging Web administration page.

Setting the IP codec set

1. Type `change ip-codec-set` *x*, where *x* is the codec set number.
2. Set the SRTP type to `1-srtp-aescm128-hmac80`, `2-srtp-aescm128-hmac32`, or `none`.

Setting the SRTP type on Communication Manager Messaging administration web interface

1. On the System Management Interface, under **Administration**, click **Messaging**.
2. Under **Switch Link Administration**, click **Switch Link Admin**.
3. In the **Media Encryption** field, select the same SRTP type that you set in the change ip-codec-set screen.
4. In the **Passphrase** field, type the password you set in the change signaling-group screen.
5. Click **Save.**

Restarting the messaging application

1. Under **Utilities**, click **Stop Messaging**.
2. After the application stops, click **Start Messaging**.

Enabling media encryption for gateway

1. Type `change media-gateway` *x*, where *x* is the number of the media gateway.
2. Enable media encryption for gateway.

Allow all non-SRTP compliant endpoints to access messaging

1. Log in to the Communication Manager server using putty.
2. Access Communication Manager server.
3. Type **`change IP codec-set`** *x*, *x* is the codec set number.
4. Set the media encryption values
    i. `1-srtp-aescm128-hmac80` or `2-srtp-aescm128-hmac32`
    ii. `none`

Note:
If you want all communication between messaging and end-points to have end-to-end audio encryption, remove the `none` entry in the Media Encryption list.

Upgrading Avaya Aura® Communication Manager Messaging

Upgrade Communication Manager R5.1.x to Communication Manager Messaging R5.2.1 on an S85XX Server

Upgrade Communication Manager R5.1.x (without Communication Manager Messaging) to Communication Manager R5.2.1. After you upgrade the server to Communication Manager

R5.2.1, follow the same upgrade procedure to install Communication Manager Messaging R5.2.1.

Upgrading Communication Manager from R5.1 to R5.2.1

1. Log in to the Maintenance Web Interface Web page.
2. Under **Server Upgrades**, click **Manage Software**.
3. On the Manage Software: Copy page, select the place to copy the installation files from and click **Continue**.
4. Select the release **05.2.1-xxx.xxx.x** and click **Continue**.
5. Select **Install one of the following releases resident on the local hard drive** and click **Continue**.
6. Choose the **5.2.1.xxx.xxx** release and click **Continue**.
7. On the Choose license source Web page, select **I want to reuse the license files from the currently active partition on this**.
8. Select **Update authentication information as well as license information**.
9. Click `Continue` and proceed to install Communication Manager.

Installing Communication Manager Messaging R5.2.1

1. Log in to the System Management Web Interface.
2. On the **Upgrade** menu, click **Manage Software**.
3. On the Manage Software: Copy Web page, select `yes` to copy the Communication Manager Messaging software.
4. Click **Continue**.
5. Proceed to install Communication Manager Messaging.

Lightweight Directory Access Protocol

Overview

Lightweight Directory Access Protocol (LDAP) is a database containing system data, subscriber data, and class-of-service assigned to a subscriber. Customers require access to the subscriber database to bulk-administer the data. Standard LDAP clients such as Microsoft Outlook are supported clients to access LDAP database.

Note:
LDAP does not include mailbox data such as messages, greetings, and announcements.

Connect to LDAP

A client can connect to LDAP in two ways:

- Anonymously
- As a Trusted Server

Connect to the LDAP database using an anonymous connection by providing an IP address and a unique name. This type of connection gets limited information from the database. A customer uses this connection to read data.

Connect to the LDAP database as a trusted Server by providing a trusted server name, IP address of the customer and password. This connection type is used to bulk-administer subscribers. Customers use the credentials provided by Avaya to get connect and get information about subscribers.

LDAP processes

The LDAP Status/Restart web page on the Messaging Administration Interface lists the processes:

- **slapd** process is responsible for the functioning of LDAP.
- **Ldapfe** process handles requests from clients about subscriber information and decides how to route requests. It runs the web administration requests for Messaging Web page users.
- **Ldapcorp** process is the same as ldapfe process except that ldapcorp facilitates external administration; customers access LDAP database from outside of the audix domain.

Checking the status of LDAP processes

1. On the System Management Interface Web page, on the **Administration** menu, click **Messaging**.
2. Under **Utilities**, click **LDAP Status / Restart**.
3. Check if all the processes are up.
4. If the processes are not up, click **Restart** to manually start the processes.

Note:
You need to restart the messaging application to start all the LDAP processes.

Login Profile Infrastructure

Overview

You can create a user-based profile and associate it to an existing Communication Manager profile or to a custom-created Communication Manager profile.

The Communication Manager Messaging application uses the user-based profiles created in Communication Manager. User-based profiles enable you to allow a user to access only a specific set of administration web pages.

For example, you can create a login account and assign it the privileged administrator profile (sa). By default, it is associated to Communication Manager profile 18. This profile provides access equivalent to the customer super user login. The unprivileged administrator profile (vm) is associated to Communication Manager profile 19. This profile provides access equivalent to the customer non-super user login.

Creating a user-based profile

1. Log in to the System Management Interface Web page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Security**, click **Web Access Mask**.
4. Click **Add**.
5. Type a profile number that you want to create for users.

   Note:
   You can create profiles 20 through 69. Profiles 0-19 are reserved.
6. Select **Create** and set all values to enable access.
7. Click **Submit**.
8. Select the profile.
9. Click **Change**.
10. By default, all web pages are selected. Select the web pages a user must have access to.
11. Click **Submit**.

    Note:
    On the Change Access Masks Web page, you can view Communication Manager Messaging web pages only if the messaging application is installed.

Assigning a profile to a user

1. Log in to the System Management Interface Web page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Security**, click **Administration Accounts**.
4. Select **Add Login**.

5. Select the type of profile.
6. Click **Submit**.

Back up and restore Communication Manager Messaging data

Overview

Communication Manager Messaging supports up to 6000 mailboxes. Back up of Communication Manager Messaging data could easily reach 50 Gigabytes or more. It would be unusual for customers to support transfers of single files of this size. Hence, Communication Manager Messaging data backup consists of multiple files, each small enough to be transferred in a customer's environment.

Supported backup methods:

- FTP
- SFTP
- SCP
- Compact PC flash card

Important:
Avaya recommends you to back up data on a network server.

Backing up Communication Manager Messaging data

Prerequisites

Network server or a PC card to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.

5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each bac up file sequentially before downloading the next backup file in the data set.

Important:

The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

Note:

Communication Manager Messaging can restore data from previous releases.

Documentation and procedure updates for Communication Manager Messaging R5.2

Change system parameters coverage

In the *system parameters coverage* section of the *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration, 03-603353 document*:

On the system-parameters coverage-forwarding screen, the **Threshold for Blocking Off_Net Redirection of Incoming Trunk Calls** field must be set to `1`.

Changing class of restriction

You need to create a hunt group for messaging before you can change the class of restriction. See, page 50 of the *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration, 03-603353 document*.

1. On the SAT screen, type **change cor** *x*, where *x* is the class of restriction number.
2. Update the **Calling Party Restriction** field to `none`. By default, the field is set to `Outward`.

Note:

You can use outward restrictions to prevent users from placing calls to the public network. These users can still place calls to other telephone users, to the attendant, and over tie trunks. If necessary, an attendant or an unrestricted telephone user can extend a call to an outside number for an outward-restricted telephone user. Calls that come into a trunk are denied if the Calling Party Restriction field on the Class of Restriction screen is set to `Outward`.

Chapter 4: Communication Manager installation on S8800 and HP DL360 G7 servers

Installing and Configuring Avaya Aura® Communication Manager

Overview

Communication Manager supports the S8800 and HP DL360 G7 servers in a 1U model. You can configure Communication Manager on an S8800 or HP DL360 G7 Server in a 1U model either in a simplex mode or a duplex mode. S8800 Server supports the US Robotics (USR) modem only. Refer to PSN001938U for additional information on modems supported by Communication Manager.

Note:

Communication Manager configured in a simplex mode on the S8800 or HP DL360 G7 Server is similar to an S85xx Server and when configured in a duplex mode is similar to an S87xx Server.

Installing Communication Manager

Prerequisites

Communication Manager Installation CD-ROM

Use a Telnet session to access the information on the CD-ROM.

1. On your Services laptop computer, click **Start** > **Run** to open the Run dialog box.
2. Type **`telnet 192.11.13.6`** and press `Enter` to view the first screen.

3. Select **Install**, ensure that **OK** is selected, and press **Enter**.
4. For HP DL360 G7 Server, on the **Server Type** screen, select **IBMX3550**, and press **Enter**.

   If the installer positively identifies the server type, the Server Type screen does not appear. The IBMX3550 allows configuration of the HP DL360 G7 Server as either simplex or duplex.

   Note:
   The **Server Type** screen only appears for the HP DL360 G7 Server.
5. On the **Select Release Version** screen, ensure that the **Build line** and **OK** are selected, and press `Enter`.
6. On the **Select Server Mode** screen, ensure that the **server mode type** and **OK** are selected, and press **Enter**.
7. Depending on the selected server duplication mode, you see different screens.
   - In simplex mode, select the **messaging option** and **OK** and press **Enter** if Communication Manager Messaging is enabled.
   - In duplex mode, select **Yes** if the server is configured for both control network A and control network B and press **Enter**.

   Note:
   After installing the Communication Manager 5.2.1 software on the server, you must install Communication Manager 5.2.1 Service Pack 6 or greater to configure the HP DL360 G7 Server.

Increase or decrease the server availability

If you configure the S8800 or HP DL360 G7 server in simplex mode and wish to increase the server availability of the server by making it a duplex server, you need to reinstall the Communication Manager software. During installation select the server mode as duplex. However, after increasing the server availability to duplex, you cannot install Communication Manager Messaging, since it cannot be installed on a server configured in duplex mode.

Likewise, if you configure the S8800 or HP DL360 G7 server in duplex mode and wish to decrease the server availability of the server by making it a simplex server, you need to reinstall the Communication Manager software. During installation select the server mode as simplex.

For hardware related information of an S8800 Server, refer to *Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager document*, 03-603444, Issue 1.

For hardware related information of an HP DL360 G7 Server, refer to *Installing the HP ProLiant DL360 G7 Server*, 03-603799.

For related tasks during installation of an S8800 or HP DL360 G7 server in simplex mode, refer to *Installing and Configuring the Avaya S8500-Series Server document*, 03-300143.

For related tasks during installation of an S8800 or HP DL360 G7 server in duplex mode, refer to *Installing and Configuring the Avaya S8700-Series Server document*, 03-300145.

Configure server

To configure S8800 or HP DL360 G7 server in simplex mode, refer to *Installing and Configuring the Avaya S8500-Series Server document*, 03-300143.

Note:

While referring to the document to configure the server, ignore the Configure RMB Web page, since it is not applicable to S8800 or HP DL360 G7 server in simplex mode. Also, since S8800 and HP DL360 G7 servers do not have the SAMP board, ignore any reference to SAMP in the document.

To configure S8800 or HP DL360 G7 server in duplex mode, refer to *Installing and Configuring the Avaya S8700-Series Server document*, 03-300145.

Note:

While referring to the document to configure the server, ignore the Configure Switches Web page, since it is not applicable to S8800 and HP DL360 G7 servers in duplex mode.

Monitor health of the server

The health of Communication Manager and the S8800 or HP DL360 G7 server can be monitored by configuring the Communication Manager heartbeat trap. The Communication Manager heartbeat trap needs an IP address to send heartbeats to SAL and a password to control access of the Communication Manager to SAL.

Administer the following parameters on Communication Manager to support the Communication Manager to SAL heartbeat:

- SAL IP address
- Community string

Accessing the Configure Health Monitor Web page

1. Open the System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Server Configuration**, click **Configure Health Monitor**.

Configuring Communication Manager and server health parameters

1. On the Configure Health Monitor Web page, complete the fields.
2. Click **Change**.

Ethernet port assignments

	Simplex		Duplex			
	Control Network A and Customer/ Corporate LAN Combined	**Independent Control Network A and Customer/ Corporate LAN**	**Control Network A and Customer/ Corporate LAN Combined**	**Independent Control Network A and Customer/ Corporate LAN**	**NIC Location of S8800 Server**	**NIC Location of HP DL360 G7 Server**
Ethernet 1 (Eth0)	Control Network A/ Customer/ Corporate LAN	Control Network A	Duplication Link		Located on mother board	Located on mother board
Ethernet 2 (Eth1)	Services Laptop		Services Laptop		Located on mother board	Located on mother board

	Simplex		Duplex			
	Control Network A and Customer/ Corporate LAN Combined	**Independent Control Network A and Customer/ Corporate LAN**	**Control Network A and Customer/ Corporate LAN Combined**	**Independent Control Network A and Customer/ Corporate LAN**	**NIC Location of S8800 Server**	**NIC Location of HP DL360 G7 Server**
Ethernet 3 (Eth2)	Not Used		Control Network A/ Customer/ Corporate LAN	Control Network A	Located on the special daughter board	Located on mother board
Ethernet 4 (Eth3)	Control Network B (if used)		Control Network B (if used)		Located on the special daughter board	Located on mother board
Ethernet 5 (Eth4)	Not Used	Customer/ Corporate LAN	Not Used	Customer / Corporate LAN	Located on the PCI Dual NIC board	Located on the PCI Dual NIC board
Ethernet 6 (Eth5)	Not Used		Not Used		Located on the PCI Dual NIC board	Located on the PCI Dual NIC board

The **Set Identities** link on the **Configure Server** Web page displays the default Ethernet ports assigned for each type of network. For the S8800 or HP DL360 G7server in duplex mode, by default, the server duplication link is assigned to Ethernet 0 port. You may choose a different Ethernet port depending on the network configuration.

Software duplication improvements

Software duplication provides memory synchronization between an active and a standby server without the need for the DAL or DAJ series of duplication cards. Software duplication is the default configuration in the S8800 1U and HP DL360 G7 servers. For software duplication, the duplication messages are sent over the server duplication TCP/IP link.

Avaya continues to support the existing hardware-duplicated S8710, S8720, and S8730 Servers. The software-duplicated S8800 1U and HP DL360 G7 servers have the same call performance as the existing hardware-duplicated S8700-Series Servers. For configuring

software duplication in the S8800 1U and HP DL360 G7 servers, Avaya recommends you to use a dedicated duplication link with the following bandwidth parameters:

- 1-Gbps raw link capacity
- 50-Mbps reserved bandwidth
- 8 ms round-trip delay, or less
- 0.1% round-trip packet loss, or less

To configure software duplication in the S8800 1U and HP DL360 G7 servers, use the **Configure Server** wizard in the System Management Interface (SMI).

IP interface for H.248 gateways

Processor Ethernet IP interface

Processor Ethernet (PE) is a logical interface in Communication Manager. No additional hardware is required to implement PE. It functions like a C-LAN and can be used instead of a C-LAN in a network environment. Network configurations can use both PE and C-LANs.

PE can be used with main and ESS servers (simplex and duplex). It allows connection to a mix of IP devices, such as H.323 telephones, trunks, gateways, SIP trunks, H.248 gateways, and selected IP connected adjuncts. The traffics supported by PE is equivalent to the traffic supported by C-LANs.

Refer to *Avaya Aura™ Communication Manager System Capacities Table for Release 5.2.1 document* to know the number of IP devices supported for S8800 and HP DL360 G7 servers in simplex and duplex mode.

Assigning IP address to Processor Ethernet

1. On the Configure Server Web page, click **Configure Interfaces**.
2. Enter the Processor Ethernet IP address.

Note:
Processor Ethernet shares the corporate LAN IP address. Each server in a duplicated system needs its own Processor Ethernet IP address.

Enabling Processor Ethernet

1. Open a SAT screen, type **`change ip-interface procr`**.
2. Tab to the **Enable Interface?** field and set it to `y`.
3. Ensure the **Allow H.323 Endpoints?** and **Allow H.248 Gateways?** fields are set to `y`.
4. Type **`Save trans`**.

Assigning IP address for Processor Ethernet on the System Management Interface

1. Open the System Management Interface (SMI).
2. On the **Installation** menu, click **Configure Server**.
3. Proceed to configure server services.
4. Click **Set Identities** to set the Ethernet port for Processor Ethernet.

   Note:
   Assign the same Ethernet port to Processor Ethernet and corporate LAN.
5. Click **Continue**.
6. On the Configure Interfaces screen, assign the IP address for the Processor Ethernet interface.

SAL integration

The default method for the S8800 and HP DL360 G7 servers to report INADS alarms and provide remote access is through the Secure Access Link (SAL) Server gateway. You can also use the USB modem instead of the default method. See the Modem support for more information. The SAL gateway is also used to monitor the Communication Manager servers'

heartbeat, to ensure that the servers are still active and provide an alarm if the Communication Manager servers are down.

You need to host the SAL functionality on a stand-alone SAL gateway or server. The USB modem uses the same modem architecture and protocols that are used on the S8300 and S87xx servers. You need to connect the USB modem to the standard USB ports on the S8800 or HP DL360 G7 server. If you use modem, service personnel cannot receive the heartbeat and detect the loss of the heartbeat. You must inform the service personnel about the loss of dial tone. If you use SAL, the SAL detects the loss of heart beat and sends an alarm to notify the service personnel that the server is down.

Note:

If you use the optional modem instead of the SAL gateway to report alarms, it is not possible to achieve the 4-nines availability on a simplex HP DL360 G7 server as there is no way to detect and report when the server is down.

Related topics:

Modem support on page 82

Configure Secure Access Link (SAL)

Configure SAL gateway

For more information about configuring SAL, see the *Secure Access Link 1.8 SAL Gateway Implementation Guide*, available as part of the software download from the Product Licensing and Delivery System (PLDS) Web site: http://plds.avaya.com.

Postinstallation

Enable alarm to INADS by way of SAL

Communication Manager generates alarms through your SAL Gateway only if Communication Manager directs its SNMP traps to the SAL Gateway.

For more information about enabling alarms for SAL gateway, see the *Secure Access Link 1.8 SAL Gateway Implementation Guide*, available as part of the software download from the Product Licensing and Delivery System (PLDS) Web site: http://plds.avaya.com.

Installation verification

Connect to the server using SAL

For more information about connecting to the server using SAL gateway, see the *Secure Access Link 1.8 SAL Gateway Implementation Guide*, available as part of the software download from the Product Licensing and Delivery System (PLDS) Web site: http://plds.avaya.com.

Chapter 5: Hardware

This chapter presents an overview of hardware additions to Release 5.2.1 of Communication Manager.

Avaya 14xx series digital telephones

The Avaya 14xx series digital telephones, namely 1408 and 1416, are Digital Communications Protocol (DCP) sets. These digital telephones can be aliased or administered as the Avaya 24xx digital telephones.

The Avaya 14xx series digital telephones have the following characteristics:

- Adjustable viewing angle
- Wall mountable
- Handset and dial pad
- Highly visible message waiting indicator
- Three or Four lines LCD
- Exit, OK, and Phone buttons to navigate the display
- Buttons for Conference, Transfer, Drop, Hold, and Redial
- Phone book or Contacts button
- 8 or 16 function keys
- Speaker, Headset, Mute buttons, each with LED indicators
- Volume up or volume down buttons for:
    - Handset
    - Headset
    - Speakerphone
- Downloadable firmware for future upgrades
- Four local softkey feature buttons
- Call Log button (to check total incoming answered, incoming unanswered, and outgoing calls)
- Message button for expedited access to voice mail
- A (Avaya Menu) button (to customize phone settings)

- Call diversion, Follow-me features
- Navigation arrows

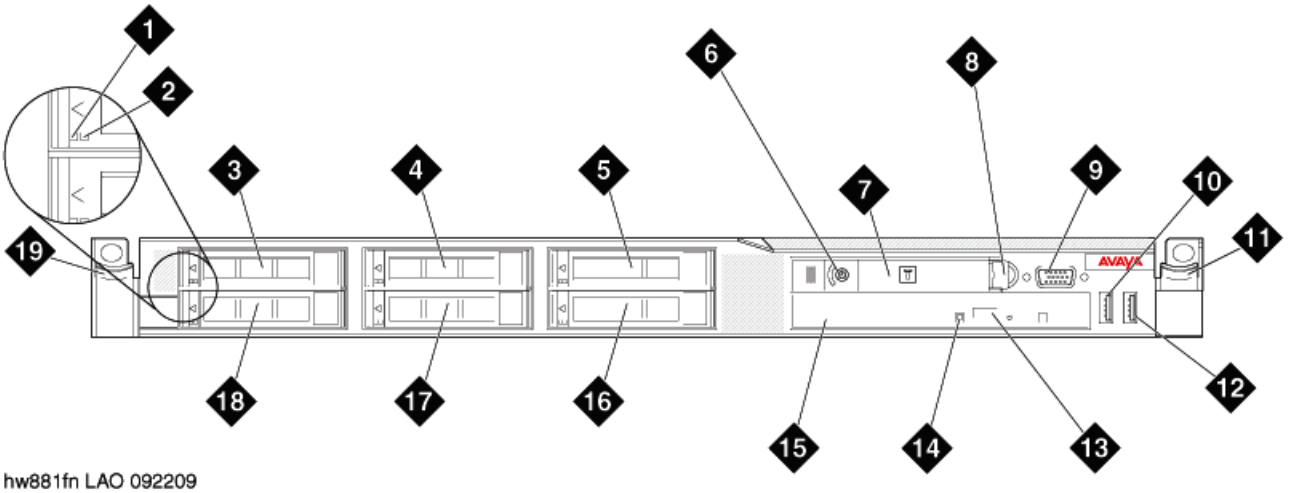
Avaya S8800 Server overview

Introduction

The Avaya S8800 Server supports several Avaya software applications. The server is available in a 1U model or 2U model and with various hardware components. The server model and specific hardware components in your server depend on the requirements of the software application that will run on the server.

Communication Manager supports the 1U model of the S8800 Server. While installing Communication Manager in simplex mode on the S8800 Server, you only use 1 S8800 Server, whereas, installing Communication Manager in duplex mode requires you to have 2 S8800 Servers.

Front of server

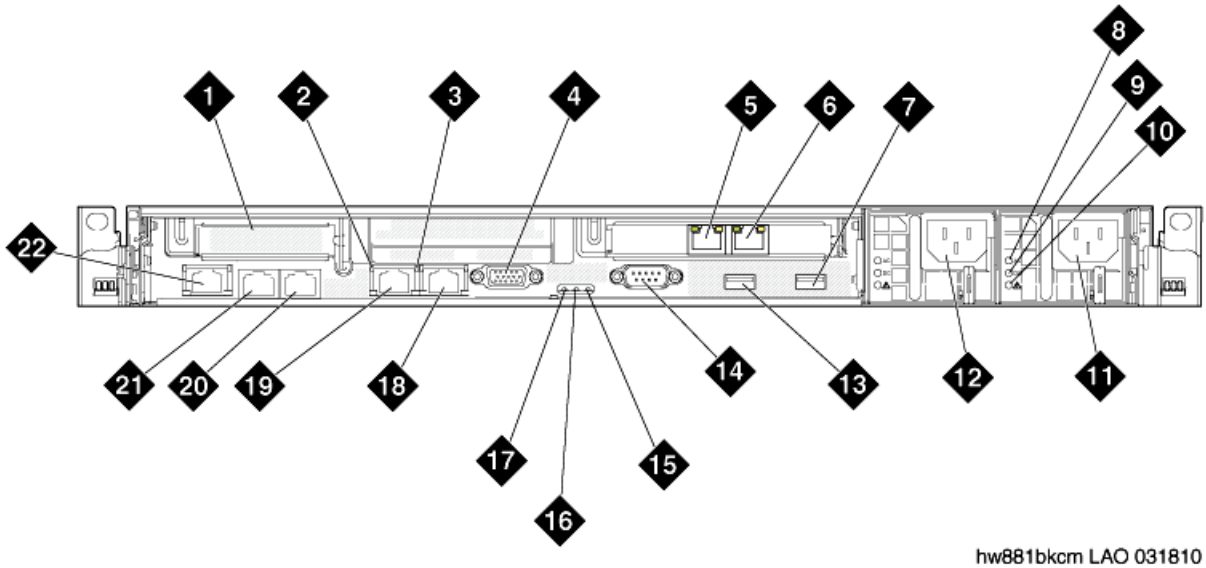


hw881fn LAO 092209

1	Hard disk drive activity LED (green)
2	Hard disk drive status LED (amber)
3	Drive bay 0
4	Drive bay 2 (unused for Communication Manager)

5	Drive bay 4 (unused for Communication Manager)
6	Power control button and LED
7	Operator information panel **Note:** The operator information panel is shown in the pushed in position.
8	Operator information panel release latch
9	Video connector
10	USB connector 1
11	Rack release latch
12	USB connector 2
13	DVD eject button
14	DVD drive activity LED
15	DVD drive
16	Drive bay 5 (Unused for Communication Manager)
17	Drive bay 3 (Unused for Communication Manager)
18	Drive bay 1
19	Rack release latch

Back of server



1	PCIe slot 1 (unused)
2	Ethernet activity LED
3	Ethernet link LED
4	Video connector
5	DUAL NIC PCI card (Ethernet connector 6 (eth5)) **Note:** Ethernet connector 6 (eth 5) is unused.
6	DUAL NIC PCI card (Ethernet connector 5 (eth4) — corporate LAN)
7	USB connector 4
8	AC power LED (green)
9	DC power LED (green)
10	Power supply error LED (amber)
11	Power supply 2 (optional redundant power supply)
12	Power supply 1 (primary power supply)
13	USB connector 3
14	Serial connector
15	System error LED (amber)
16	System locator LED (blue)
17	Power LED (green)
18	Ethernet connector 2 (eth 1) (Services port)
19	Ethernet connector 1 (eth 0) (Duplication link if configuration is duplicated server)
20	Daughter card (Ethernet connector 4 (eth 3) - Control Network B)
21	Daughter card (Ethernet connector 3 (eth 2) - corporate LAN and or Control Network A if configuration is duplicated server)
22	System management Ethernet connector (IMM)

Note:

Hardware label for Ethernet ports on the server is called Ethernet connectors. Communication Manager software refers to Ethernet ports as eth.

Server specifications

Type	Description
Dimensions	Height: 43 mm (1.69 inches, 1U) Depth: 711 mm (28 inches) Width: 440 mm (17.3 inches)
Weight	Maximum weight: 15.4 kg (34 lb.) when fully configured.
Heat output	Approximate heat output: • Minimum configuration: 662 Btu per hour (194 watts) • Maximum configuration: 1400 Btu per hour (400 watts) Heat output varies depending on the number and type of optional features that are installed and the power-management optional features that are in use.
Acoustic noise emissions	Declared sound power, operating: 6.1 bel The sound levels were measured in controlled acoustical environments according to the procedures specified by the American National Standards Institute (ANSI) S12.10 and ISO 7779 and are reported in accordance with ISO 9296. Actual sound-pressure levels in a given location might exceed the average values stated because of room reflections and other nearby noise sources. The declared sound-power levels indicate an upper limit, below which a large number of computers will operate.
Electrical input requirements	• Sine-wave input (47–63 Hz) required • Input voltage low range: - Minimum: 100 V AC - Maximum: 127 V AC • Input voltage high range: - Minimum: 200 V AC - Maximum: 240 V AC • Input kilovolt-amperes (kVA), approximately: - Minimum: 0.194 kVA - Maximum: 0.700 kVA
Front connectors	• Two USB • Video
Back connectors	• Two Ethernet (RJ 45). Optionally, two or four additional Ethernet. • Serial

Type	Description
	• Two USB • Video • Systems management Ethernet (IMM)

Server components

Component	Minimum specification	Upgrade options based on product requirements
Microprocessor	One Intel E5520 quad core, 2.26 GHZ processor	No additional options
Memory	4 GB of 1333 Mhz, fully-buffered DDR-3 RDIMMs (Two 2GB DIMMs):	12 GB of 1333 Mhz, fully-buffered DDR-3 RDIMMs memory **Note:** You must upgrade to 12 GB memory to support Communication Manager Release 6.x.
Media drive	DVD-R/W SATA slimline	No additional options
Hard disk drive expansion bays	Six 2.5-inch hot-swap SAS hard disk drive bays	No additional options
Hard disk drive	Two 146 GB SAS 2.5" 10K RPM (RAID 1) hard drives	Three 146 GB SAS 2.5" 10K RPM (RAID 5) hard drives **Note:** You must upgrade to three hard drives to support Communication Manager Release 6.x.
RAID controllers	ServeRAID-MR10i RAID SAS adapter that provides RAID level 1 or 5. Includes 256 MB cache module and battery for write cache	No additional options

Component	Minimum specification	Upgrade options based on product requirements
PCI expansion slots	Two PCI Express x16 Gen 2 slots: • Slot 1 supports a low profile DUAL NIC card (half height, half-length cards) • Slot 2 supports full height, half-length cards	No additional options
Hot-swap fans	Six	No additional options
Power supply	One 675W, 12V AC power supply	Redundant 675W, 12V AC power supply
Video controller	Integrated Matrox G200 (two analog ports, one front and one back, that can be connected at the same time) The maximum video resolution is 1280 x 1024 at 75 Hz. • SVGA compatible video controller • DDR2 250 MHz SDRAM video memory controller • Avocent Digital Video Compression • Video memory is not expandable	No additional options

Environmental requirements

Server status	Air temperature	Maximum Altitude	Relative humidity
Server on	10 to 35º C (50 to 95º F) at altitude of up to 914.4 m (3,000 feet)	2,133 m (7,000 feet)	8% to 80%

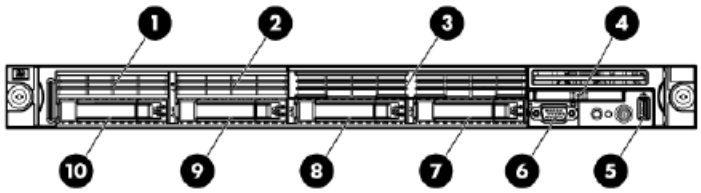
Server status	Air temperature	Maximum Altitude	Relative humidity
	10 to 32º C (50 to 90º F) at altitude of 914.4 m to 2,133 m (3,000 to 7,000 feet)		
Server off	10°C to 43°C (50.0°F to 109.4°F)	2,133 m (7,000 feet)	8% to 80%

HP ProLiant DL360 G7 1U server overview

Introduction

The Avaya Common Servers category includes the HP ProLiant DL360 G7 1U server that supports several Avaya software solutions, some requiring additional hardware and memory requirements beyond the standard configuration. This book covers the standard configuration only—consult specific Avaya product documentation for application-specific or solution-specific server configurations.

Front of server



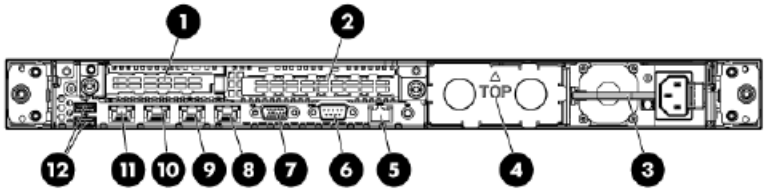
Note:

Servers ship with 2–4 hard disk drives, depending upon product requirements.

No.	Description
1	Not present
2	Not present
3	DVD-RW
4	HP Systems Insight Display

No.	Description
5	Front USB connector
6	Video connector
7	Hard drive bay 4
8	Hard drive bay 3
9	Hard drive bay 2
10	Hard drive bay 1

Back of server



Reference	Description
1	Ethernet connector 5 (eth 4) and Ethernet connector 6 (eth 5) – located on PCI Dual NIC board
2	Slot 2 PCIe2 x16 (16, 8, 4, 2, 1), 75W +EXT 75W* **Note:** Servers might ship with a PCI card installed, depending upon product requirements.
3	Power supply bay 1 (populated)
4	Power supply bay 2
5	iLO 3 connector
6	Serial connector
7	Video connector
8	Ethernet connector 4 (eth 3)
9	Ethernet connector 3 (eth 2)
10	Ethernet connector 2 (eth 1)
11	Ethernet connector 1 (eth 0)
12	USB connectors (2)

*This expansion slot provides 75 W of power to an adapter, with an additional 75 W of power supplied by external power.

Server specifications

Baseline configurations and options for the HP DL360 G7 server:

Component	Minimum specification	Upgrade options based on product requirements
DL360 G7	1U chassis, dual socket	No additional options supported.
Processor	Simplex configuration: Intel E5620 Quad Core / 2.4 GHz (Westmere), 1 CPU, 3 memory channels per CPU with up to 3 RDIMMs per channel **Note:** Simplex server with the single E5620 2.4 GHz processor can be used in a duplex server configuration. Duplex configuration: Intel X5670 six Core / 2.93 GHz (Westmere), 1 CPU, 3 memory channels per CPU with up to 3 RDIMMs per channel	N/A
Memory	6 x 2GB DDR3 RDIMMs (1333 MHz) for a total of 12GB	N/A
HW RAID 1	P410i RAID controller with 256MB cache and battery backup. Optioned as RAID 5	N/A
Disk drive	146GB SAS 2.5" 10K RPM 6G DP Hard Drive. Base configuration: 272 total: RAID 5, 3 x 146GB drives	N/A
NICs	6 NIC ports — HP NC382T PCI Express Dual Port Gigabit NIC expansion card (Broadcom 5709 silicon) in addition 4 integrated ENET Gigabit NIC ports	N/A
PCI slots	Two PCI-Express Gen 2 expansion slots: (1) full-length, full-height slot and (1) low-profile slot (1-FL/FH x 16 PCIe & 1-LP x 8 PCIe Riser	N/A
Removable media	Slim line SATA DVD-RW optical drive (used in all Avaya configurations)	No additional options supported.

Component	Minimum specification	Upgrade options based on product requirements
Power supply	Single 460 W hotplug AC power supply	Redundant 460 W power supply available.
Fans	3 fan modules (fan redundancy standard)	No additional options supported.
Additional items	1 front USB, 2 back USB, 1 internal USB	

Environmental specifications

The HP DL360 G7 environmental specifications are listed below:

Specification	Value
Temperature range	**Note:** All temperature ratings shown are for sea level. An altitude derating of 1°C per 300 m (1.8° per 1,000 ft.) to 3048 m (10,000 ft.) is applicable. No direct sunlight allowed.
Operating	10°C to 35°C (50°F to 95°F)
Shipping	-40°C to 70°C (-40°F to 158°F)
Maximum wet bulb temperature	28°C (82.4°F)
Relative humidity (noncondensing)	**Note:** Storage maximum humidity of 95% is based on a maximum temperature of 45° C (113°F). Altitude maximum for storage corresponds to a pressure minimum of 70 kPa.
Operating	10% to 90%
Non-operating	5% to 95%

Physical specifications

The HP DL360 G7 physical specifications are listed below:

Specification	Value
Dimensions	Height: 4.32 cm (1.70 in)

Specification	Value
	Width: 42.62 cm (16.78 in)
	Depth: 69.53 cm (27.38 in)
Weight (maximum; two processors, two power supplies, eight hard disk drives)	15.97 kg (35.20 lb)
Weight (minimum; one processor, one power supply, no hard drives)	14.51 kg (32.00 lb)
Weight (no drives installed)	14.06 kg (31.00 lb)

Modem support

Communication Manager supports all of the following USB modems:

- Old MultiTech
- New MultiTech
- US Robotics (USR) modem

For new sales only the USR modem is available. Customers can reuse the MultiTech modem. The following table describes the modem specifications:

Terminology	Modem Description	Manufacturer's Product Name
Old MultiTech	USB MODEM V.92 56K RHS	MT5634 USB (discontinued)
New MultiTech	USB MODEM MT9234ZBA V.92 56K RHS	MT9234ZBA-USB
USR Modem	USB MODEM USR5637-OEM 56K ROHS 6	USR5637-OEM

References

For more information on HP DL360 G7 server, see the following:

- *Installing the HP ProLiant DL360 G7 Server*, 03-603799.
- *Maintaining and Troubleshooting the HP ProLiant DL360 G7 Server*, 03-603803.

Chapter 6: Documentation and procedure updates

The Communication Manager documents (maintenance alarms, commands, procedures, hardware guide, administrator guide, etc.) are not being updated for this release.

This chapter describes the following updates and additions for Communication Manager Release 5.2.1 which will not be documented elsewhere for this release.

Adding New Hardware for Avaya Servers and Gateways

The following change applies to the *Adding New Hardware for Avaya Servers and Media Gateways*, 03-300684:

Downloading Reliable Data Transport Tool

1. Log on to http://support.avaya.com.
2. In the **InSite Knowledge Management** search box, type “Reliable Data Transport Client/Server Tool” including the quotation marks.
3. Press `Enter`.
4. In the search results, click the appropriate Communication Manager Downloads link of 08/26/2010.
5. On the download page, click **Reliable Data Transport Client/Server Tool V2.0** of 31-Aug-2005.
6. Click **RDTT_R2.1.exe**.
7. Click **Save**.
8. Make note of the default download directory.

   -or-

   Browse to the appropriate directory.

9. Click **Save**.
10. Click **Run**.

Note:
To view and save the accompanying `ReadMe` file, select **RDTT_Readme_2.1.doc**.

Administering Network Connectivity

The following change applies to the *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504:

Reviewing the network region administration

Reference 6.0 version – page 172, after step 4, the following steps are added:

1. Enter `list ip-network-region igar-dpt` to see the IP Network Regions IGAR-DPT screen, which gives an overview of fields related to the Inter-Gateway Alternate Routing and Dial Plan Transparency features.
2. Ensure that the IGAR and DPT parameters are administered according to your design.

Administration for the Avaya G450 Media Gateway

The following changes apply to the *Administration for the Avaya G450 Media Gateway*, 03-602055:

DHCP server CLI configuration

Reference 5.2 version – Chapter 18, Step 3, page 484: The combined number of IP addresses in all pools must not exceed 1024 addresses, not 256 addresses.

Administrator guide

The following changes apply to the *Administering Avaya Aura™ Communication Manager*, 03-300509:

Avaya Site Administration

Reference 5.2 version – page 20 and page 545, first paragraph, the following sentence is removed: ASA is available in several languages.

PE Interface configuration

The description of PE Interface Acceptance Test is added under the PE Interface configuration section.

PE Interface acceptance test

If the main servers are duplicated and PE interface is not used (that is, no ESS server is provided and no IP endpoints are controlled by PE interface), PE interface should not be enabled. The Status Summary page should show that Processor Ethernet connection is not functional on both servers, and PE priority is set to IGNORE for both servers.

If the Status Summary page does not provide the information stated above, you should verify the following:

- For Communication Manager 5.0 and 5.1 releases, the PE Interface should be set to **UNUSED** on the Set Identities page. The PE Interchange Priority should be set to **IGNORE** on the Configure Interfaces page.
- For Communication Manager 6.0 and later releases, the Functional Assignment for eth0 should not include Processor Ethernet on the Network Configuration page. The PE Interchange Priority should be set to **IGNORE** on the Duplication Parameters page.

If the main servers are duplicated and PE interface is used (that is, ESS server is provided or IP endpoints are controlled by the PE interface, or both ESS server is provided and IP endpoints are controlled by the PE interface), PE Interface on both the main server and the ESS server should be enabled. The Status Summary page should show that Processor Ethernet connection is functional on both servers, and PE Priority is set to same value (but not IGNORE) on both servers.

If the Status Summary page does not provide the information stated above, you should verify the following:

- For Communication Manager 5.0 and 5.1 releases, PE Interface should be set to one of the Ethernet interfaces on the Set Identities page, and PE Interchange Priority should be set to the same value (but not IGNORE) on the Configure Interfaces page on both servers.
- For Communication Manager 6.0 and later releases, Functional Assignment for eth0 should include Processor Ethernet on the Network Configuration page, and the PE Interchange Priority should be set to the same value (but not IGNORE) on the Duplication Parameters page on both servers.

If the main server or ESS server is duplicated, the Current Alarms page or the **`almdisplay -v shell`** command should not show any active _PE alarms for up to 15 minutes after both servers have been running as an active or standby pair.

SIP Telephones

In addition to 9600SIP and 4600SIP, Communication Manager 5.2 and later offers four new options for native SIP administration. These options are:

- 9620SIP
- 9630SIP
- 9640SIP
- 9650SIP

If you change currently administered SIP phones to the new options, or if you use the newly administered SIP phones with the specific options, H.323 soft phones cannot work. The endpoint must be a SIP phone to administer natively.

Telephone Feature Buttons

An Instant Transfer button is added to the Telephone Feature Buttons table.

Button Label	Button Name	Description
Instant Transfer	Inst-trans	An Instant Transfer button does an instant transfer by performing an immediate unsupervised transfer to the button's administered destination. The Instant Transfer button is intended for transfer to Polycom room systems, which are capable of hosting a conference and auto-answering calls as well. The Instant Transfer button is not limited to video set-types; however, it may be useful on other set-types as well.

Conversion of servers and gateways

The following changes apply to the *Converting Avaya Servers and Media Gateways*, 03-602884:

Suppress alarming

Reference 5.2 version – pages 217, 220, 227, and 247, step four is removed: Log off and close the dialog box.

Denial Events

The following changes apply to the *Avaya Aura™ Communication Manager Denial Events*, 03-602793:

Call Processing Denial Events

Event Types 5035 is a continuation of call processing-generated denial events, and is listed in the following table:

Event Type	Event Description, as it appears on the event log	Explanation	Event Data 1	Event Data 2
5035	NCR:Xfer/cnf drp inv fail	The Network Call Redirection invocation failed for station transfer or conference drop.	response type	response

Feature Description and Implementation

The following changes apply to the *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555–245–205:

Administering Extension to Cellular

Setting up One-X Server integration

1. Set up SIP signaling group and trunk group between Communication Manager and one-X Server.
2. Provision users with Communication Manager extensions on one-X Server.
3. Provisioned users will have ONE-X mapping(s) acquired against their extensions on Communication Manager. Verify using **`list off-pbx-telephone station-mapping`** or **`display off-pbx-telephone station-mapping`** command.

Call forward override

If the Call Forward Override feature is turned on, and a call terminates at an already visited station for that call as a part of the call forward chain, the call is not forwarded. Instead, the call continuously rings at that station to avoid loops while traversing the chained call forward path.

For example, Station A has activated call forward feature to Station B, Station B to Station C, and Station C to Station D. In this case, if Station A gets an incoming call and forwards the call to Station B, then Station B forwards the call to Station C, and Station C forwards the call to Station D. Eventually the call is answered by Station D, which transfers the call to Station A. The call continuously rings at Station A and is not forwarded to Station B.

Condition Codes

The following condition codes are added to the existing condition codes table:

Condition codes	Description
O	Identifies CDR records for all calls in which URI was used as dialed digits.
P	Identifies CDR records for all calls in which SA8957 PIN code for Private Calls was used.

Enhanced Redirection Notification

For Enhanced Redirection Notification, you must enable at least one of the Redirection Notification options listed in the Feature-Related System Parameters screen. For example, if you disable all the redirection notification options, all the notifications appear on the IP (H.323) telephones. The system does not check the notifications to be displayed when you disable all the options. However, if you activate **Do Not Distrub (DND) notification** field, only the DND notification appears on the endpoints. This is because the system checks the displayed notifications only when you enable at least one of the options.

Interactions for Bridged Call Appearance

Emergency calls

If a user dials an emergency call from a bridged appearance, the Calling Party Number that is sent to the public safety answering point is based on the extension of the physical telephone from which the call is made.

Note:

To set up an emergency call, you must administer at least one call appearance as a primary call appearance.

Interactions for Station Security Code

This section provides information about how the Station Security Code feature interacts with the other features on the system. Use this information to ensure that you receive the maximum benefits of Station Security Code in any feature configuration.

You may need a Station Security Code to use the following system features and capabilities:

- Call Forwarding
- Demand Printing
- Extended User Administration of Redirected Calls
- Enterprise Mobility User
- Extension to Cellular
- Leave Word Calling (LWC)
- Personal Station Access (PSA)
- Posted Messages
- Station Lock

- Security Violation Notification
- Terminal Self-Administration
- User Change Coverage
- Voice Message Retrieval

Interactions for Whisper Paging

Service Observing

When a service observer is active on a call, whisper page to an observing or observed station is denied.

System requirements for EMU

The following description is added to the existing System requirements for EMU section:

For optimal performance and feature functionality EMU requires,

- Private numbering administration supporting UDP dialing between enterprise sites.
- The EMU visiting user is able to dial directly the EMU home user using UDP dialing.
- The EMU home user is able to dial directly the EMU visiting user using UDP dialing.
- All locations dialing. If per location dialing or partition group route administration is configured, Communication Manager does not support EMU. If an EMU user is assigned to a location or is reached through partition group routing, EMU registration is not allowed.

Hardware Description and Reference

The following changes apply to the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207:

TN791 analog guest line (16 ports)

A note that mentions TN791 circuit pack is not used in a G650 Media Gateway is removed, as G650 Media Gateway supports TN791 circuit pack.

Maintenance Alarms

The following changes apply to the *Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300430:

CONFIG (System Configuration)

Error log entries and recommended actions

Reference 6.0 version – page 290, the note about Error Type 257 is modified to 'less than 75% of the overall trunk group capacity is available.'

disable synchronization-switch

The **`disable synchronization-switch`** command is renamed as **`disable synchronization`**.

enable synchronization-switch

The **`enable synchronization-switch`** command is renamed as **`enable synchronization`**.

IP Signaling Group Far-End Status Test (#1675)

The description of the IP Signaling Group Far-End Status Test is updated as follows:

This test validates that you can use the trunks on this signaling group. If the test fails, the affected signaling channel is taken out of service and an alarm is raised. Once the test passes, the primary is put back in service and the alarm is retired.

SIP-SGRP (SIP Signaling Group)

Error log entries and recommended action

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Recommended Action
258	17	IP Signaling Group Far-End Status Test (#1675)	MIN	OFF	

Note:
Error Type 258: Primary signaling link is unavailable.

Maintenance Commands

The following changes apply to the *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431:

AAR and ARS Digit Analysis Table

The following Action/Object is added to the AAR and ARS Digit Analysis Table under the Administration Screen Reference section.

Action/Object	Qualifier
list aar route-chosen	dialed number [partition *n*] [schedule]

disable synchronization-switch

The **`disable synchronization-switch`** command is renamed as **`disable synchronization`**.

enable synchronization-switch

The **`enable synchronization-switch`** command is renamed as **`enable synchronization`**.

list ars route-chosen

The following field description is added in the list ars route-chosen field descriptions table.

Field	Description
Actual Outpulsed Digits by Preference	Digits outpulsed when you choose each of the preferences in the chosen route pattern.

Reports

The following change apply to the *Avaya Aura™ Communication Manager Reports*, 555-233-505:

AAR or ARS Route Chosen reports

Reference 6.0 version – pages 55 and 56, the following field description is added in the existing field description table:

Field	Description
Actual Outpulsed Digits by Preference	Digits outpulsed when you choose each of the preferences in the chosen route pattern.

Attendant and Maintenance Status report

The following description is added to the existing Attendant and Maintenance Status report section:

To ensure that the authorized users log into the system, you must click **Cancel** to log off from the SAT screen after running the **`monitor system view1`** and **`monitor system view2`** commands.

Screen Reference

The following changes apply to the *Avaya Aura™ Communication Manager Screen Reference*, 03-602878:

AAR and ARS Digit Analysis Table

The * as a wildcard character is not a valid entry for the **Dialed String** field on the AAR and ARS Digit Analysis Table screens.

AAR and ARS Digit Conversion Table

The * as a wildcard character is not a valid entry for the **Matching Pattern** field on the AAR and ARS Digit Conversion Table screens.

Agent LoginID

The description of the **Security Code** field on the Agent LoginID screen is modified.

Security Code

The four-digit station security code (password) for the Demand Print messages feature.

Attendant Console

The description of the **Security Code** field on the Attendant Console screen is modified.

Security Code

The station security code required by the SoftConsole IP attendant.

BCMS/VuStats Service Level

Provides for hunt groups or Vector Directory Numbers (VDNs) with an acceptable service level. An acceptable service level defines the number of seconds within which a call must be answered to be considered acceptable.

Dial Plan Analysis Table

The description of the **Percent Full** field on the Dial Plan Analysis Table screen is modified as follows:

Percent Full

Valid Entry	Usage
0 to 100	The percentage of system memory resources that have been allocated for the dial plan currently used. For details on the system memory resources, see *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.

Extension only label for Team button on 96xx H.323 terminals

Available only if the **Team Btn Display Name** for the Class of Restriction is enabled.

Valid entries	Usage
y	For 96xx H.323 telephones, displays the station extension without the team button label. 96xx H323 firmware version 2.0 or greater is recommended as it provides a special icon for team buttons. This field does not impact label customizations.
n	For 96xx H.323 telephones, displays the station extension with the team button label.

External Ringing for Calls with Trunks

Specifies ringing behavior on external trunk calls that are transferred or conferenced by stations or attendants, or extended by the attendant to an on-switch extension.

Valid Entry	Usage
all-calls	All external trunk calls that are transferred or conferenced (either locally or remotely) receive external ringing.
local-only	External trunk calls that are transferred or conferenced locally receive external ringing.
none	External ringing does not apply to external trunk calls that are transferred or conferenced.
remote-only	External trunk calls that are transferred or conferenced remotely receive external ringing. This is the default value.

Feature-Related System Parameters

The following fields are added on the Feature-Related System Parameters screen:

Restrict Calls

Indicates the type of calls to block first during overload traffic conditions on the system.

Valid Entry	Usage
stations-first	Deny new traffic generated by internal stations, allowing inbound calls only. This works best in call center environments.
all-trunks-first	Deny all incoming trunk calls and does not block station off-hook.
public-trunks-first	Deny incoming calls on ISDN public trunks and analog CO trunks.

Zip Tone Burst For Call master Endpoints

Valid entry	Usage
double	When the station set type is a Callmaster series, Communication Manager retains existing operation which applies the following to ACD agents: • two bursts of zip tone for auto-answer ACD calls • two burst of ICI tweedle-dee tone for non-ACD auto-answer calls This is the default value.
single	Communication Manager eliminates the 2nd burst of zip/ICI tone reducing time for agent to start conversation with the caller and possibility of the agent and the caller hears open mike background noise between

Valid entry	Usage
	the first and second tones. Use with a Callmaster station type when the agent can always hear enough of the single burst auto-answer to recognize that a call is being delivered.

Hunt Group

The following changes are made related to the Hunt Group screen:

- The **Acceptable Service Level (sec)** field is removed from the Hunt Group screen.
- The description of the **Security Code** field on the Hunt Group screen is modified.
- The **Service Level Target (% in sec)** field and the **Interruptible Aux Threshold** field descriptions are modified.

Interruptible Aux Threshold

Valid Entry	Usage
service-level-target	Specifies which threshold triggers an event to interrupt agents interruptible for a skill. The Interrupt Aux feature is triggered if the service level drops below the administered percent calls in the specified seconds. For example, if the target is 90% calls in 30 seconds, the Interruptible Aux feature is triggered if the measure drops to 89% calls in 30 seconds.
none	Interruptible Aux is not active for this hunt group.

Security Code

The four-digit station security code (password) for the Demand Print messages feature.

Service Level Target (% in sec)

Appears when the **ACD** field and the **Measured** field is not blank, and when one or more of the following features are active:

- **BCMS/VuStats Service Level** field on the System Parameters Customer-Options screen is active and the **Measured** field is set to internal or both. The service level target in seconds is used as the acceptable level for reporting the percentage of calls answered within the specified time. The percentage can be set to the default of 80%.
- Business Advocate on the System Parameters Customer-Options screen is active. The service level target in seconds is used for the Business Advocate Service Level

Supervisor service level objective. This service level target can also be used for the dynamic percentage adjustment when the **Dynamic Threshold Adjustment** field on the Hunt Group screen is y and for the dynamic percent adjustment when the **Group Type** field on the Hunt Group screen is pad and the **Dynamic Percent Adjustment** field on the Hunt Group screen is set to y.

- **Service Level Target** field appears when the **Group Type** field on the Hunt Group screen is slm, and on the System Parameters Customer-Options screen, the Service Level Maximizer is active, and the Business Advocate customer option license is not active. In this case the setting is also used as the service level target to trigger SLM.
- **Interruptible Aux Threshold** field on the Hunt Group screen is set to service-level-target. The Interrupt Aux feature is triggered if the service level drops below the administered percent calls in the specified seconds.

Valid Entry	Usage
1 to 99 (percentage)	The percentage component of the service level target. The default value is 80%.
1 to 9999 (time in seconds)	The time component of the service level target. The default value is 20 seconds.

Incoming Call Handling Treatment

In addition to predefined Services/Features, any user-defined Facility Type of 0 (feature), 1 (service), 2 (incoming), or 3 (outgoing) on the Network Facilities screen is allowed. For a Service/Feature defined as Type 2, the Incoming Call Handling Treatment screen determines which incoming calls are assigned to this Service/Feature. See the description of the Network Facilities screen for details.

Service type 2 is useful when creating a user-defined service on the ISDN Network Facilities screen. A user defined service with Facility Type 2 allows special routing on the Incoming Call Handling Treatment Table as well as Min/Max usage restrictions on the Usage Allocation table.

Facility type 3 is useful when creating a user-defined service for outgoing calls on ISDN cbc trunk groups. If a user-defined service with Facility Type 3 is used for a route pattern preference, the outgoing SETUP message will not contain an NSF IE, and the call will be counted in the corresponding user-defined service entry in the Usage Allocation table.

Incoming Dialog Loopbacks

Appears on the Signaling Group screen when the **Group Type** field is sip.

Valid entries	Usage
allow	Communication Manager software connects the call and allows the SIP trunks to remain in the looparound connection. Avaya recommends that if the trunk group controlled by this SIP signaling group is used for IGAR calls, the value be set to allow.
eliminate	Communication Manager software connects the call and eliminates the SIP trunks from the looparound connection. The default value is eliminate.

ISDN Numbering Calling Party Number Conversion for Tandem Calls

Note:

The Calling Party Number Conversion for Tandem Calls screen does not update the Calling Party Number in an NCA-TSC SETUP message. Such updates might come in a QSIG Message Waiting Indication message from a Voice Mail adjunct.

Location

The description of the **Location** field on the AAR and ARS Digit Analysis Table, AAR and ARS Digit Analysis Table, and Dial Plan Analysis Table screens is modified as follows:

Valid Entry	Usage
1 to 250	(Depending on your server configuration, see *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.) The location of the endpoint that is dialing the digits. See the Location sections in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for the other ways to assign a location, and for a list of features that use location.
all	Phones dialing from this location use the entries in the Call Type Digit Analysis Table. If there are matching entries in the telephone's location, those entries are used. If there are no matching entries in the phone's location, the Communication Manager tries the entries in location all. If the **Multiple Locations** field is disabled, the value of the **Location** field is all.

Location Parameters

Off-PBX Feature Name Extension Set

Valid Entry	Usage
0 to 10 for a medium configuration 1 to 99 for a large configuration	Feature Name Extension (FNE) set that should be used for location based call routing.
blank	Default FNE set is used. This is the default.

Long Distance Access Code

Valid Entry	Usage
0 to 9	The long distance access code you want the system to prefix to the telephone number. Accepts up to five digits.
blank	Not administered. This is the default.

Numbering-Public/Unknown Format and Numbering-Private Format

Overview of Numbering-Public/Unknown Format and Numbering-Private Format screens

In Communication Manager 5.2.1 and later releases, you must administer the extensions of all calls traversing SIP trunks in the appropriate private and public numbering tables on the Numbering-Public/Unknown Format and Numbering-Private Format screens. You must also configure the private and public numbering tables in the Numbering-Public/Unknown Format and Numbering-Private Format screens for all extensions. You must populate the calls to extensions terminating on a SIP integrated Modular Messaging in the appropriate Numbering-Public/Unknown Format or Numbering-Private Format screens, and do not configure a prefix for the SIP trunk group by which the Modular Messaging is integrated.

off-pbx-telephone station-mapping

On the Off-PBX Telephone Station-Mapping screen, page 2, the **Location** field is modified.

Location

Valid entry	Usage
1 to 50 for medium configurations 1 to 250 for large configurations	The location value for each administered OPS, PBFMC, SPFMC or PVFMC application. • For a DCP deskset, the location of the media gateway • For an IP deskset, the location of the network region belonging to the deskset
blank	Trunk location is used for the outgoing calls from Off-PBX endpoints and location of station is used for incoming calls to Off-PBX endpoints. Blank is the default.

Outgoing Trunk Disconnect Timer (minutes)

The **Outgoing Trunk Disconnect Timer (minutes)** field is moved from page 2 of the **Class of Restriction (COR)** screen to page 3 of the COR screen.

Percent Full

The description of the **Percent Full** field on the AAR and ARS Digit Analysis Table, AAR and ARS Digit Conversion Table, Precedence Routing Digit Analysis Table, and Toll Analysis screens is modified as follows:

Value	Comments
0 to 100	The percentage of system memory resources that have been used by the table. For details on the system memory resources, see *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.

Personal CO Line Group

The description of the **Security Code** field on the Personal CO Line Group screen is modified.

Security Code

The station security code that users must dial to retrieve voice messages and to use the Demand Print Message feature. Accepts from three to eight digits.

QSIG to DCS TSC Gateway

The following note is added to the description of the **Subscriber Number** field on the QSIG to DCS TSC Gateway screen.

Subscriber Number

Note:

If the Subscriber Number is local, the form does not send any DCS messages over the listed Sig Grp/TSC Index. Therefore, you can put a block entry like '2xxx' with the understanding that if extension 2001 is local, no DCS message will be sent.

Refresh Terminal Parameters Access Code

Feature Access Code (FAC) is used to request a refresh of the terminal parameters on a telephone that supports downloadable parameters. This FAC is used after a DCP telephone is installed or replaced to ensure that all the terminal parameters, including button labels, are sent to the telephone.

Shared UUI Feature Priorities

ASAI

User information from Adjunct/Switch Applications Interface (ASAI).

Valid Entry	Usage
1 to 7	Level of priority, with 1 being the highest. Default priority is 1.
blank	This field's information is not forwarded.

Collected Digits

Digits collected from caller (not including dial-ahead digits).

Valid Entry	Usage
1 to 7	Level of priority, with 1 being the highest. Default priority is 5.
blank	This field's information is not forwarded.

Held Call UCID

The unique tag for the last call that was put on hold by the Automatic Call Distribution (ACD) agent placing this call to another system. This Universal Call ID (UCID) can be used to identify the original or parent call that may eventually be placed into conference or transferred to the other system. This element is required for cradle-to-grave tracking with Avaya IQ release 5.0 and later.

Valid Entry	Usage
1 to 7	Level of priority, with 1 being the highest. The UCID included in the element with default priority 2 is the tag for a new call placed by the agent while the original call is on hold. Default priority is 7.
blank	This field's information is not forwarded.

In-VDN Time

Number of seconds the call has spent in vector processing.

Valid Entry	Usage
1 to 7	Level of priority, with 1 being the highest. Default priority is 3.
blank	This field's information is not forwarded.

Other LAI Information

Includes the time stamp of when the call entered the current queue, the call’s priority level in its current queue, and the type of interflow.

Valid Entry	Usage
1 to 7	Level of priority, with 1 being the highest. Default priority is 6.
blank	This field's information is not forwarded.

Universal Call ID

A unique tag that identifies the call that this message is being sent for and the other information included in the User-User-Information (UUI).

Valid Entry	Usage
1 to 7	Level of priority, with 1 being the highest. Default priority is 2.
blank	This field's information is not forwarded.

VDN Name

Name of the active VDN (also called LAI DNIS).

Valid Entry	Usage
1 to 7	Level of priority, with 1 being the highest. Default priority is 4.
blank	This field's information is not forwarded.

Station

Security Code

The security code required by users for specific system features and functions are as follows:

- Extended User Administration of Redirected Calls
- Personal Station Access
- Redirection of Calls Coverage Off-Net
- Leave Word Calling
- Extended Call Forwarding
- Station Lock
- Voice Message Retrieval
- Terminal Self-Administration
- Enterprise Mobility User
- Extension to Cellular
- Call Forwarding
- Posted Messages

- Security Violation Notification
- Demand Printing

The required security code length is administered system wide.

Survivable COR

Sets a level of restriction for stations to be used with the survivable dial plan to limit certain users to only to certain types of calls. You can list the restriction levels in order from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by PIM module of the Integrated Management to communicate with the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for Standard Local Survivability (SLS) on the H.248 gateways.

Available for all analog and IP station types.

Valid Entries	Usage
emergency	This station can only be used to place emergency calls.
internal	This station can only make intra-switch calls. This is the default.
local	This station can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.
toll	This station can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables.
unrestricted	This station can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users.

Survivable GK Node Name

Any valid previously-administered IP node name. Identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the H.248 gateways. When a valid IP node name is entered into this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP stations register with Communication Manager, this list is sent down in the registration confirm message. This allows the IP station to use the IP address of this Survivable Gatekeeper as the call controller of last resort.

If blank, there are no external gatekeeper nodes within a customer's network. This is the default value.

Available only if the station type is an H.323 station for the 46*xx* or 96*xx* models.

Survivable Trunk Dest

Designates certain telephones as not being allowed to receive incoming trunk calls when the Media Gateway is in survivable mode. This field is used by the PIM module of the Integrated Management to successfully interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the H.248 gateways.

Available for all analog and IP station types.

Valid Entry	Usage
y	Allows this station to be an incoming trunk destination while the Media Gateway is running in survivability mode. This is the default.
n	Prevents this station from receiving incoming trunk calls when in survivable mode.

Survivable ARS Analysis Table

The Survivable ARS Analysis Table screen is not a valid screen and will be removed from the *Avaya Aura™ Communication Manager Screen Reference*.

Terminating Extension Group

The description of the **Security Code** field on the Terminating Extension Group screen is modified.

Security Code

The four-digit station security code (password) for the Demand Print messages feature.

Trunk Group

Analog Loss Group

Determines which administered two-party row in the loss plan applies to this trunk group if the call is carried over an analog signaling port in the trunk group.

Valid Entry	Usage
1 to 17	The index into the loss plan and tone plan. If values are administered other than in between 6 and 10 or 15 and 17, a warning message displays stating that the loss group may not be appropriate for this trunk group.

Digital Loss Group

Valid Entry	Usage
1 to 19	Determines which administered two-party row in the loss plan applies to this trunk group if the call is carried over a digital signaling port in the trunk group. If values other than 18 or between 11 and 15 are administered, a warning message displays stating that the loss group may not be appropriate for this trunk group.

Uniform Dial Plan Table

The **Acceptable Service Level (sec)** field is not a valid field on the Uniform Dial Plan Table screen and will be removed from the *Avaya Aura™ Communication Manager Screen Reference*.

Usage Allocation Enhancements

Enables the user to use user-defined entries for the incoming and outgoing ISDN calls independent of the NSF value. The Usage Allocation Enhancements feature lets the user administer the non-unique Facility Type and Facility Coding combinations. It also enables the customer to reserve a minimum number of trunk members for the incoming and outgoing calls at all times.

Note:

The Usage Allocation Enhancements feature is helpful outside the US, where the default Network Facilities available in the system are not very useful.

Use Trunk COR for Outgoing Trunk Disconnect

The **Use Trunk COR for Outgoing Trunk Disconnect** field is renamed to **Use Trunk COR for Outgoing Trunk Disconnect/Alert** on page 6 of the Feature-Related System Parameters screen.

Uniform Dial Plan Table

The description of the **Percent Full** field on the Uniform Dial Plan Table screen is modified as follows:

Percent Full

Displays the percentage (0 to 100) of the memory resources allocated for the uniform dial plan data that are currently being used. For details on the system memory resources, see *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.

VDN Override for ISDN Trunk ASAI Messages

The **VDN Override for ISDN Trunk ASAI Messages** field is renamed to **VDN Override for ASAI Messages** on page 2 of the Vector Directory Number screen and the field description is also modified.

VDN Override for ASAI Messages

Determines if the active VDN is sent as the called number for ISDN Trunk ASAI messages. When **Meet-me Conferencing** is disabled, this field follows VDN override rules when the system changes the “active” VDN for a call. The “active” VDN is the VDN receiving the call and will be changed to a routed-to VDN if **Allow VDN Override** is enabled. Available only if **ASAI Link Core Capabilities** is enabled for the system.

Valid Entry	Usage
n	The “Called Number” information is sent for the “Call Offered”, “Alerting”, “Queued”, and “Connect” ASAI event notification messages. The adjunct-request message is always the called VDN extension in the Called Number IE sent in the incoming ISDN SETUP message or the local call’s called number and does not change after routing to the called VDN and subsequent routed-to VDNs.
ISDN Trunk	When an incoming ISDN trunk call is routed to this VDN, the “Called Number” information sent in the ASAI event and “Adjunct Route Request” ASAI messages is the “active VDN” extension. This extension becomes associated with the call based on the VDN Override rules. This option does not apply to local/internal calls.
all	The active VDN is used for the called number for all types of calls to the VDN, including local/internal calls as well as external incoming ISDN trunk calls.

Server Alarms

The following changes apply to the *Avaya Aura™ Communication Manager Server Alarms*, 03-602798:

Login Alarms

The Login alarm Event ID 4 is replaced with the 10, 11, 12 and 13 Event IDs. The description of the Event IDs are mentioned in the following table:

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
10, 11, 12, and 13	MIN	"Login for [linux] – failed – password check" 1. A login to a server's Linux command line failed. Verify the alarm, either from the: • System Management Interface, by selecting **Current Alarms** • Linux command line, by entering `almdisplay -v` 2. Since mis-typing a login sequence usually causes this alarm, enter `almclear -n #id` to clear the alarm. 3. If this alarm is perceived as a security threat (often due to its persistence or frequent recurrence), notify the customer.

Upgrade, Migration, and Conversion of servers and gateways

The following changes apply to Upgrading, Migrating, and Converting Avaya Servers and Gateways 5.0, 03-300412:

Suppressing alarming

Caution:
Suppress alarming during the upgrade. If you do not suppress alarming, the system can generate alarms, resulting in unnecessary trouble tickets.

1. Access the command line interface of the server using Telnet or an SSH client application like PuTTY.
2. Enter `192.11.13.6`.
3. Log in as `craft`.
4. Enter `almsuppress -t time`, where time is the length of time that the alarms are suppressed up to 120 minutes (2 hours). Press `Enter` to suppress both dial-out and SNMP alarms.
   The system displays the following message:

   ```
   Alarm is suppressed. 120 minutes left.
   ```

Using the Avaya Enterprise Survivable Servers

The following change apply to the Using the Avaya Enterprise Survivable Servers, 03-300428:

ESS requirements

You can use S8400 Server as a main server and an Enterprise Survivable Server (ESS) with the following limitations:

The sum of the following three components must not be greater than 1500:

- The number of H.323 Signaling Groups administered on the main server.
- The number of H.323 Trunk members administered on the main server.
- The number of H.323 IP endpoints that registers with the S8400 ESS.

The total number of H.323 IP endpoints on the system can be larger than the number that registers with the S8400 ESS if the limitations are met.

If the server exceeds the above limits and the S8400 ESS becomes active, server does not register all the IP endpoints. The H.323 Signaling Groups and the H.323 Trunk members first

use the administered number of IP User Records from the pool of 1500. Any remaining IP User Records are used for registering IP endpoints.

For example, if the main server has a total of 1000 H.323 Signaling Groups and Trunk members, 500 IP stations can register with the S8400 ESS. The main server does not experience any limitations due to the S8400 ESS.

Note:

The above limits are not enforced by Communication Manager software.

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

Z