Administering Avaya Aura™ Communication Manager

Release 6.0
03-300509
Issue 6
June 2010

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

Chapter 1: Introduction

Overview

Avaya Aura™ Communication Manager is the centerpiece of Avaya applications. Running on a variety of Avaya S8XXX Servers, and providing control to Avaya Media Gateways and Avaya communications devices, Communication Manager can be designed to operate in either a distributed or networked call processing environment.

Communication Manager carries forward all of a customer's current DEFINITY capabilities, plus offers all the enhancements that enable them to take advantage of new distributed technologies, increased scalability, and redundancy. Communication Manager evolved from DEFINITY software and delivers no-compromise enterprise IP solutions.

Communication Manager is an open, scalable, highly reliable and secure telephony application. The software provides user and system management functionality, intelligent call routing, application integration and extensibility, and enterprise communications networking.

Purpose of this book

This book describes the procedures and screens used in administering the most recent release of Communication Manager running on any of the following:

- Avaya S8XXX Servers
  - S8300D, S8510, or S8800 server
- Avaya S8XXX Servers configured as a Survivable Remote Server (Local Survivable Processor)
- Avaya media gateways
  - G250, G350, G430, G450, or G700 Media Gateways

Newer releases of Communication Manager contain all the features of prior releases.

Related resources

Note:

For information about the screens referenced in this book, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

The following documents provide additional information.

- *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504
- *ATM Installation, Upgrades, and Administration using Avaya Communication Manager*, 555-233-124
- *Avaya Application Solutions: IP Telephony Deployment Guid*e, 555-245-600
- *Avaya Business Advocate User Guide*, 07-300653
- *Avaya Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568
- *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780
- *Avaya Communication Manager Advanced Administration Quick Reference*, 03-300364
- *Avaya Communication Manager Basic Administration Quick Reference*, 03-300363
- *Avaya Communication Manager Basic Diagnostics Quick Reference*, 03-300365
- *Avaya Remote Feature Activation (RFA) User Guide*, 03-300149
- *Avaya Toll Fraud and Security Handbook*, 555-025-600
- *Converged Communications Server Installation and Administration*, 555-245-705
- *DEFINITY Communications Systems Generic 2.2 and Generic 3 Version 2 DS1/CEPT1/ISDN PRI Reference*, 555-025-107
- *DEFINITY Enterprise Communications Server Release 1.1 Getting Started with the Avaya R300 Remote Office Communicator*, 555-233-769
- *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205
- *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207
- *Installation, Upgrades and Additions for Avaya CMC1 Media Gateways*, 555-233-118
- *Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300430
- *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431

- *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300432
- *Avaya Aura™ Communication Manager Overview*, 03-300468
- *Avaya Aura™ Communication Manager Reports*, 555-233-505
- *Avaya Aura™ Communication Manager Screen Reference*, 03-602878
- *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511
- *Avaya Aura™ Communication Manager Survivable Options*, 03-603633
- *What's New in Avaya Aura™ Communication Manager, Avaya Servers and Media Gateways for Release 6.0*, 03-601528

For documents not listed here, go to http://www.avaya.com. Select **Support** and then **Product Documentation**.

Send us your comments

Avaya appreciates any comments or suggestions that you might have about this product documentation. Send your comments to the Avaya documentation team.

Chapter 2: System Basics

Logging into the System

You must log in before you can administer your system. If you are performing remote administration, you must establish a remote administration link and possibly assign the remote administration extension to a hunt group before you log in. The members of this hunt group are the extensions of the data modules available to connect to the system administration terminal. For information about setting up remote administration, contact your Avaya technical support representative. When not using the system, log off for security purposes.

Logging in for remote administration

Procedure

1. Dial the Uniform Call Distribution (UCD) group extension number.

   Note:

   The UCD group extension number is assigned when you set up remote administration.

   - If you are off-premises, use the Direct Inward Dialing (DID) number, a Listed Directory Number (LDN) (you must use a telephone), or the trunk number dedicated to remote administration.
   - If you are on-premises, use an extension number.

     If you dialed a DID number, dedicated trunk number, or extension, you receive data tone or visually receive answer confirmation.

     If an LDN was dialed, the attendant will answer.

     i. Ask to be transferred to the UCD group extension number.

        You receive data tone or visually receive answer confirmation.

     ii. Transfer the voice call to your data terminal.

   The Login prompt displays.

2. Complete the steps for Logging into the System.

For information about setting up remote administration, contact your Avaya technical support representative.

See also Enhancing System Security. For a complete description of the Security Violation Notification feature, see Security Violation Notification in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Accessing the Avaya S8XXX Server

To administer an Avaya S8XXX Server, you must be able to access it. Personal computers and services laptop computers equipped with an SSH client (PuTTY) or Avaya Site Administrator (ASA), and a Web browser are the primary support access for system initialization, aftermarket additions, and continuing maintenance.

You can access an Avaya S8XXX Server in one of three ways:

- directly
- remotely over the customer's local area network (LAN)
- over a modem for Communication Manager Release 5.2 or earlier

A direct connection and over the customer's LAN are the preferred methods. Remote access over a modem is for Avaya maintenance access only.

Accessing the Avaya S8XXX Server Directly — connected to the services port

Before you begin

Enable IP forwarding to access System Platform through the services port.

Procedure

1. Open the MS Internet Explorer browser.

   Microsoft Internet Explorer version 7.0 is supported.
2. In the **Location/Address** field, type the IP address of the Communication Manager server.
3. Press `Enter`.
4. When prompted, log in to administer the Avaya S8XXX Server and the features of Communication Manager.

Enabling IP forwarding to access System Platform through the services port

About this task

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the Avaya S8XXX Server Directly — connected to the customer network

Procedure

1. Open the MS Internet Explorer browser.

   Microsoft Internet Explorer version 7.0 is supported.
2. In the **Location/Address** field, type the active server name or IP address.
3. Press `Enter`.
4. When prompted, log in to administer the Avaya S8XXX Server and the features of Avaya Communication Manager.

   You can also connect directly to an individual server using its name or IP address.

Accessing the Avaya S8XXX Server remotely over the network

About this task

You can access the Avaya S8XXX Server from any computer connected through the LAN. To access either server, use the IP address assigned to the server you want to access. You can also use the active server address to connect automatically to the server that is active. Once connected, you can administer the server using three tools:

- Web interface for server-specific administration and call processing features.
- Avaya Site Administration for Communication Manager (Only available on the active Communication Manager server).
- An SSH client, like PuTTY, and a configured IP address for the Communication Manager server.

Using Avaya Site Administration

Avaya Site Administration features a graphical user interface (GUI) that provides access to SAT commands as well as wizard-like screens that provide simplified administration for frequently used features. You can perform most of your day-to-day administration tasks from this interface such as adding or removing users and telephony devices. You can also schedule tasks to run at a non-peak usage time.

This software must be installed on a computer running a compatible Microsoft Windows operating system. Once installed, it can be launched from a desktop icon.

Installing Avaya Site Administration

Before you begin

If you do not have ASA on your computer, make sure your personal computer (PC) or laptop first meets the following minimum requirements:

Table 1: Site Administration: Microsoft Windows client computer requirements

Component	Required	Comments
Operating System	Microsoft Windows XP Professional with Service Pack 3, Microsoft Windows 2003 Standard Edition server with Service Pack 2, Microsoft Windows 2003 Enterprise Edition server with Service Pack 2,	

Component	Required	Comments
	Microsoft Windows Vista Business (32-bit and 64-bit editions) with Service Pack 2, Microsoft Windows Vista Enterprise (32-bit and 64-bit editions) with Service Pack 2, Microsoft Windows 7, Microsoft Windows 2008 Standard Edition server with Service Pack 2, or Microsoft Windows 2008 Enterprise Edition server with Service Pack 2	
Processor	latest Intel or AMD-based processors	
Hard Drive	1 GB	Required to install all of the client components.
Memory	512 MB RAM	
Monitor	SVGA 1024 X 768 display	
Network Connectivity	TCP/IP 10/100 Network Card	
Modem	56 Kbps Modem	May be required for remote access to the computer.
Other Software	Internet Explorer 6.0 with Service Pack 1 or Service Pack 2, Internet Explorer 7.0 Service Pack 1, or Internet Explorer 8.0, Mozilla Firefox 3.0 or 3.5 and Java Runtime Environment 1.6.0_16.	Required to access the Integrated Management Launch Page and Web-based clients.

About this task

Install ASA on your computer using the Avaya Site Administration CD. Place the ASA CD in the CD-ROM drive and follow the installation instructions in the install wizard.

ASA supports a terminal emulation mode, which is directly equivalent to using SAT commands on a dumb terminal or through an SSH session. ASA also supports a whole range of other features, including the graphically enhanced interface (GEDI) and Data Import. For more information see the Help, Guided Tour, and Show Me accessed from the ASA Help menu.

Starting Avaya Site Administration

Procedure

1. Start up ASA by double-clicking the ASA icon, or click **Start** >**Programs** > **Avaya Site Administration**.
2. In the **Target System** field, use the pull-down menu to select the desired system.

3. Click **Start GEDI**.
   You now are connected to the desired system.

Configuring Avaya Site Administration

When Avaya Site Administration is initially installed on a client machine, it needs to be configured to communicate with Communication Manager on the Avaya S8XXX Server.

When you initially run ASA, you are prompted to create a new entry for the switch connection. You are also prompted to create a new voice mail system if desired.

Logging in with Access Security Gateway

Access Security Gateway (ASG) is an authentication interface used to protect the system administration and maintenance ports and logins associated with Avaya Communication Manager. ASG uses a challenge and response protocol to validate the user and reduce unauthorized access.

You can administer ASG authentication on either a port type or login ID. If you set ASG authentication for a specific port, it restricts access to that port for all logins. If you set ASG authentication for a specific login ID, it restricts access to that login, even when the port is not administered to support ASG.

Authentication is successful only when Avaya Communication Manager and the ASG communicate with a compatible key. You must maintain consistency between the Access Security Gateway Key and the secret key assigned to the Communication Manager login. For more information about ASG, see Using Access Security Gateway (ASG).

Before you can log into the system with ASG authentication, you need an Access Security Gateway Key, and you need to know your personal identification number (ASG). The Access Security Gateway Key must be pre-programmed with the same secret key (such as, ASG Key, ASG Passkey, or ASG Mobile) assigned to the Avaya Communication Manager login.

Verify that the **Access Security Gateway (ASG)** field on the System-Parameters Customer Options (Optional Features) screen is set to y. If not, contact your Avaya representative.

Logging in with ASG

Procedure

1. Enter your login ID.

The system displays the challenge number (for example, 555-1234) and system Product ID number (for example, 1000000000). The Product ID provides Avaya Services with the specific identifier of your Avaya MultiVantage communications application.

2. Press **ON** to turn on your Access Security Gateway Key.
3. Type your PIN.
4. Press **ON**.
   The Access Security Gateway Key displays an 8 digits challenge prompt.
5. At the challenge prompt on the Access Security Gateway Key, type the challenge number without the "-" character (for example, 5551234) from your screen.
6. Press **ON**.
   The Access Security Gateway Key displays a response number (for example, 999-1234).
7. At the response prompt on your terminal, type the ASG response number without the "-" character (for example, 9991234).
8. Press `Enter`.
   The Command prompt displays.

Note:

If you make 3 invalid login attempts, the system terminates the session. For more information, see the appropriate maintenance book for your system.

Login messages

Two messages may be displayed to users at the time of login.

- The `Issue of the Day` message appears prior to a successful login. In general, use the `Issue of the Day` to display warnings to users about unauthorized access. The client that is used to access the system can affect when, how, and if the user sees the `Issue of the Day` message.
- The `Message of the Day` (MOTD) appears immediately after a user has successfully logged in. In general, use the `Message of the Day` to inform legitimate users about information such as upcoming outages and impending disk-full conditions.

Using the system default Issue of the Day

About this task

The Communication Manager file `/etc/issue.avaya` contains sample text that may be used for the `Issue of the Day` message.

Procedure

1. Log into the Communication Manager server.
2. At the CLI enter the following commands:
   - `cp /etc/issue.avaya /etc/issue`
   - `cp /etc/issue.avaya /etc/issue.net`

Setting Issue of the Day and Message of the Day

About this task

For more detailed information on setting login messages and interaction with individual access services, see the *Communication Manager Administrator Logins* White Paper on http://support.avaya.com.

In general, to administer the Issue of the Day and the Message of the Day, use /bin/vi or /usr/share/emacs to perform the following edits:

1. Configure `etc/pam.d/mv-auth` to include issue PAM module.
2. Edit `/etc.issue and /etc.issue.net` (if using telnet) to include the text for the Issue of the Day.
3. Edit `etc/motd` to include the text for the Message of the Day.

The following strings is not permitted in a Message of the Day (case sensitive). When searching for strings, white space and case are ignored.

- `[513]` used by FPM, CMSA, VAM
- `513]` used by connect2
- `]` used by MSA
- `Software Version` used by ASA
- `Login:`
- `Password:`
- `Challenge:`
- `ogin`

- `ogin:`
- `incorrect logoin`
- `assword`
- `hallenge`
- `SAT`
- `SAT` cannot be executed on a standby server

Logging off the System

For security, log off any time you leave your terminal. If you use terminal emulation software to administer Communication Manager, log off the system and exit the emulation application before switching to another software package.

Logging off the System-Instructions

Procedure

1. Type `logoff`.
2. Press `Enter`.

   If the Facility Test Call or Remote Access features are administered, **Alarm origination** is disabled, or if you have busied out resources or active minor or major alarms, a security screen displays. You might want to take appropriate action (for example, disable these features or address any alarms) before you log off.

   If none of the above special circumstances exist, the system logs you off.
3. At the **Proceed with Logoff** prompt, type y to log off.

   If you log off with alarm origination disabled and the system generates an alarm, Avaya support services will not receive any notification of the alarm. For more information about alarms, see the maintenance book for your system.

Administering User Profiles and Logins

Authentication, Authorization and Accounting (AAA) Services allows you to store and maintain administrator account (login) information on a central server. Login authentication and access authorization is administered on the central server.

For details on administering user profiles and logins, see AAA Services in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, and

Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431.

Establishing Daylight Savings Rules

Avaya Communication Manager allows you to set the daylight savings time rules so that features, such as time-of-day routing and call detail recording (CDR), adjust automatically to daylight savings time. The correct date and time ensure that CDR records are correct. You can set daylight savings time rules to transition to and from daylight savings time outside of normal business hours, so the number of affected CDR records is small.

You can set up 15 customized daylight savings time rules. This allows Communication Manager administrators with servers in several different time zones to set up a rule for each. A daylight savings time rule specifies the exact time when you want to transition to and from daylight savings time. It also specifies the increment at which to transition (for example, 1 hour).

Establishing Daylight Savings Rules - Instructions

Procedure

1. Type `change daylight-savings-rules`.
2. Press `Enter`.

   Rule 1 applies to all time zones in the U.S. and begins on the first Sunday on or after March 8 at 2:00 a.m. with a 01:00 increment. Daylight Savings Time stops on the first Sunday on or after November 1 at 2:00 a.m., also with a 01:00 increment (used as a decrement when switching back to Standard time. This is the default.

   The increment is added to standard time at the specified start time and the clock time shifts by that increment (for example, for 01:59:00 to 01:59:59 the clock time shows 01:59 and at 02:00 the clock shows 03:00).

   On the stop date, the increment is subtracted from the specified stop time (for example, for 01:59:00 to 01:59:59 the clock time shows 01:59 and at 02:00 the clock shows 01:00).

   > **Note:**
   >
   > You cannot delete a daylight savings rule if it is in use on either the Locations or Date and Time screens. However, you can change any rule except rule 0 (zero).

   The Daylight Savings Rules screen appears.

3. To add a Daylight Savings Time rule, complete the **Start** and **Stop** fields with the day, month, date, and time you want the system clock to transition to Daylight Savings Time and back to standard time.
4. Press `Enter` to save your changes.

   Note:

   Whenever you change the time of day, the time zone, or daylight savings rules, you must reboot the server for the changes to take effect. See the documentation for your system for information on rebooting the server.

Displaying daylight savings time rules

Procedure

1. Type `display daylight-savings-rules`.
2. Press **Enter**.
   The Daylight Savings Rules screen appears. Verify the information you entered is correct.

Setting Time of Day Clock Synchronization

Time of Day Clock Synchronization enables a server to synchronize its internal clock to UTC time provided by Internet time servers. Avaya uses the LINUX platform system clock connected to an Internet time server to provide time synchronization. The interface for these systems is web-based.

Setting the system date and time

The system date and time is entered through System Platform. For information on how to set up the date and time, see the Configuring date and time section.

Related topics:

Configuring date and time on page 585

Displaying the system date and time

Procedure

1. Type `display time`.
2. Press `Enter`.
   The Date and Time screen displays. Verify the information you entered is correct.

Related topics

See Establishing Daylight Savings Rules for more information about setting system time.

For additional information, see *Avaya Call Center Release 4.0 Automatic Call Distribution (ACD) Guide, 07-600779*.

Using the Bulletin Board

Avaya Communication Manager allows you to post information to a bulletin board. You can also display and print messages from other Avaya server administrators and Avaya personnel using the bulletin board. Anyone with the appropriate permissions can use the bulletin board for messages. Only one user can post or change a message at a time.

Whenever you log in, the system alerts you if you have any messages on the bulletin board and the date of the latest message. Also, if Avaya personnel post high-priority messages while you are logged in, you receive notification the next time you enter a command. This notification disappears after you enter another command and reoccurs at login until deleted by Avaya personnel.

You maintain the bulletin board by deleting messages you have already read. You cannot delete high-priority messages. If the bulletin board is at 80% or more capacity, a message appears at login indicating how much of its capacity is currently used (for example, 84%). If the bulletin board reaches maximum capacity, new messages overwrite the oldest messages.

Note:

The bulletin board does not lose information during a system reset at level 1. If you save translations, the information can be restored if a system reset occurs at levels 3, 4, or 5.

Displaying messages

Procedure

1. Type `display bulletin-board`.
2. Press `Enter`.
   The Bulletin Board screen displays.

Posting a message

About this task

In our example, we post a message to the bulletin board about a problem with a new trunk group, and an Avaya representative replies to our message.

Procedure

1. Type `change bulletin-board`.
2. Press `Enter`.
   The Bulletin Board screen displays.

   There are three pages of message space within the bulletin board. The first page has 19 lines, but you can only enter text on lines 11-19. The first 10 lines on page 1 are for high-priority messages from Avaya personnel and are noted with an asterisk (*). The second and third pages each have 20 lines, and you can enter text on any line. The system automatically enters the date the message was posted or last changed to the right of each message line.
3. Type your message.

   You can enter up to 40 characters of text per line. You also can enter one blank line. If you enter more than one blank line, the system consolidates them and displays only one. The system also deletes any blank line if it is line one of any page. You cannot indent text on the bulletin board. The **Tab** key moves the cursor to the next line.
4. Press `Enter` to save your changes.

Deleting messages

Procedure

1. Type `change bulletin-board`.
2. Press `Enter`.
   The Bulletin Board screen appears.
3. Enter a space as the first character on each line of the message you want to delete.
4. Press `Enter`.
5. Press `Enter` to save your changes.

Save translations

Use `save translation` to commit the active server translations (volatile) in memory to a file (non-volatile). It either completes or fails. For Linux platforms, the translation file is copied to the standby server by a filesync process.

All translation data is kept in volatile system memory or on the hard drive during normal operation. In the event of a power outage or certain system failures, data in memory is lost. `Save translation` stores on disk the translation data currently in memory.

When a SAT user issues save translation on a duplicated system, translations are saved on both the active and standby servers. If an update of the standby server is already in progress, subsequent save translation commands fail with the message `save translations has a command conflict`.

`Save translation` will not run and an error message appears when:

- translation data is being changed by an administration command.
- translations are locked by use of the Communication Manager Web interface Pre-Upgrade Step.

Run `save translation` as part of scheduled background maintenance or on demand.

For information on the `save translation` command and the command syntax descriptions, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

Perform Backups

Information on performing backups to your system can be found in the *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300432.

Chapter 3: System Planning

Communication Manager consists of hardware to perform call processing, and the software to make it run. You use the administration interface to let the system know what hardware you have, where it is located, and what you want the software to do with it. You can find out which circuit packs are in the system and which ports are available by entering the command list configuration all. There are variations on this command that display different types of configuration information. Use the help function to experiment, and see which command works for you.

System Configuration

Planning Your System

The System Configuration screen shows all the boards on your system that are available for connecting telephones. You can see the board number, board type, circuit-pack type, and status.

At a very basic level, Communication Manager consists of hardware to perform call processing, and the software to make it run. You use the administration interface to let the system know what hardware you have, where it is located, and what you want the software to do with it.

You can find out which circuit packs are in the system and which ports are available by entering the command list configuration all. There are variations on this command that display different types of configuration information. Use the help function to experiment, and see which command works for you.

To view a list of port boards on your system: Type `list configuration port-network`. Press `Enter`.

The System Configuration screen shows all the boards on your system that are available for connecting telephones, trunks, data modules and other equipment. You can see the board number, board type, circuit-pack type, and status of each board’s ports. The u entries on this screen indicate unused ports that are available for you to administer. These might also appear as p or t, depending on settings in your system.

You will find many places in the administration interface where you are asked to enter a port or slot. The port or slot is actually an address that describes the physical location of the equipment you are using. A port address is made up of four parts:

cabinet the main housing for all the server equipment. Cabinets are numbered starting with 01.

carrier the rack within the cabinet that holds a row of circuit packs. Each carrier within a cabinet has a letter, A to E.

slot the space in the carrier that holds an individual circuit pack. Slots are numbered 01-16.

port the wire that is connected to an individual piece of equipment (such as a telephone or data module). The number of ports on a circuit pack varies depending on the type.

So, if you have a single-carrier cabinet, the circuit pack in slot 06 would have the address 01A06. If you want to attach a telephone to the 3rd port on this board, the port address is 01A0603 (01=cabinet, A=carrier, 06=slot, 03=port).

Viewing a list of port boards

Procedure

1. Go to the administration interface.
2. Enter `list configuration port-network.`

   The System Configuration screen shows all the boards on your system that are available for connecting telephones, trunks, data modules and other equipment. You can see the board number, board type, circuit-pack type, and status of each board’s ports. The u entries on this screen indicate unused ports that are available for you to administer. These entries might also appear as p or t, depending on settings in your system.

Understanding equipment addressing

Where addressing is used

You will find many places in the administration interface where you are asked to enter a port or slot. The port or slot is actually an address that describes the physical location of the equipment you are using.

Address format

A port address is made up of four parts:

- cabinet — the main housing for all the server equipment. Cabinets are numbered starting with 01.
- carrier — the rack within the cabinet that holds a row of circuit packs. Each carrier within a cabinet has a letter, A to E.

- slot — the space in the carrier that holds an individual circuit pack. Slots are numbered 01-16.
- port — the wire that is connected to an individual piece of equipment (such as a telephone or data module). The number of ports on a circuit pack varies depending on the type.

Example

So, if you have a single-carrier cabinet, the circuit pack in slot 06 would have the address 01A06. If you want to attach a telephone to the 3rd port on this board, the port address is 01A0603 (01=cabinet, A=carrier, 06=slot, 03=port).

Dial plan

Understanding the Dial Plan

What the dial plan does

Your dial plan tells your system how to interpret dialed digits. For example, if you dial 9 on your system to access an outside line, it is actually the dial plan that tells the system to find an external trunk when a dialed string begins with a 9.

The dial plan also tells the system how many digits to expect for certain calls. For example, the dial plan might indicate that all internal extensions are 4-digit numbers that start with 1 or 2. Let us take a look at an example dial plan so you'll know how to read your system's dial plan.

Dial plan access table

The Dial Plan Analysis Table defines the dialing plan for your system. The Call Type column in the Dial Plan Analysis Table indicates what the system does when a user dials the digit or digits indicated in the Dialed String column. The Total Length column indicates how long the dialed string will be for each type of call.

Dial plan parameters table

The Dial Plan Analysis Table works with the Dial Plan Parameters Table for fully defining your dial plan. The Dial Plan Parameters Table allows you to set system-wide parameters for your dial plan, or to define a Dial Plan Parameters Table per-location.

Uniform dial plan

To Administer a Uniform Dial Plan, you can set up a Uniform Dialing Plan that can be shared among a group of servers. For more information, see *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Displaying your dial plan

Procedure

1. Go to the administration interface.
2. Enter `display dialplan analysis` or `display dialplan analysis location n`, where n represents the number of a specific location.
3. Press `Enter` to save your changes.

Modifying your dial plan

Procedure

1. Go to the administration interface.
2. Enter **`change dialplan analysis`** or `display dialplan analysis location n` where n represents the number of a specific location. Press `Enter`
3. Move the cursor to an empty row.
4. Type `7` in the **Dialed String** column. Press `Tab` to move to the next field.
5. Type `3` in the **Total Length** column. Press `Tab` to move to the next field.
6. Type `dac` in the **Call Type** column.
7. Press `Enter` to save your changes.

Adding Extension Ranges

About this task

You might find that as your needs grow you want a new set of extensions. Before you can assign a station to an extension, the extension must belong to a range that is defined in the dial plan.

In this example, we will add a new set of extensions that start with 3 and are 4 digits long (3000 to 3999).

Procedure

1. Go to the administration interface.

2. Enter `change dialplan analysis` or `change dialplan analysis location n`, where n represents the number of a specific location. Press `Enter`.
3. Move the cursor to an empty row.
4. Type `3` in the **Dialed String** column. Press `Tab` to move to the next field.
5. Type `4` in the **Total Length** column. Press `Tab` to move to the next field.
6. Type `ext` in the **Call Type** column.
7. Press `Enter` to save your changes.

Multi-location dial plan

Definition

When a customer migrates from a multiple independent node network to a single distributed server whose gateways are distributed across a data network, it might initially appear as if some dial plan functions are no longer available.

The multi-location dial plan feature preserves dial plan uniqueness for extensions and attendants that were provided in a multiple independent node network, but appear to be unavailable when customers migrate to a single distributed server. This feature is available beginning with Communication Manager, release 2.0.

Example

For example, in a department store with many locations, each location might have had its own switch with a multiple independent node network. The same extension could be used to represent a unique department in all stores (extension 123 might be the luggage department). If the customer migrates to a single distributed server, a user could no longer dial 123 to get the luggage department in their store.

The user would have to dial the complete extension to connect to the proper department. Instead of having to dial a complete extension, the multi-location dial plan feature allows a user to dial a shorter version of the extension. For example, a customer can continue to dial 123 instead of having to dial 222-123.

Communication Manager takes leading digits of the location prefix and adds some or all of its leading digits (specified on the Uniform Dial Plan screen) to the front of the dialed number. The switch then analyzes the entire dialed string and routes the call based on the administration on the Dial Plan Parameters and Dial Plan Analysis screens.

Note:

Before you can administer the multi-location dial plan feature, the **Multiple Locations** field on the System Parameters Customer-Options (Optional Features) screen must be enabled. To check if this is enabled, use the `display system-parameters customer-options` command. The **Multiple Locations** field is on page 3 of the Optional Features screen. Set this field to y.

Location numbers

How equipment gets location numbers

Equipment gets location numbers as follows:

- IP telephones indirectly obtain their location number. A location number is administered on the IP Network Region screen that applies to all telephones in that IP region.
- Non-IP telephones and trunks inherit the location number of the hardware they are connected to (for example, the cabinet, remote office, or media gateway).
- IP trunks obtain their location from the location of its associated signaling group. Either direct administration (only possible for signaling groups for remote offices), or the ways described for IP telephones, determines the location.

Location administration

A location number is administered on the IP Network Region screen that applies to all telephones in that IP region. If a Location field is left blank on an IP Network Region screen, an IP telephone derives its location from the cabinet where the CLAN board is that the telephone registered

Prepending the location prefix to dialed numbers

About this task

Complete the following steps to assign the location prefix from the caller's location on the Locations screen.

Procedure

1. Go to the administration interface.
2. Enter **`change uniform-dialplan`**.
3. Enter the prefix in the in the **Insert Digits** field.
4. Press `Enter` to save your changes.

   The system adds some or all of its leading digits (specified on the Uniform Dial Plan screen) to the front of the dialed number. The switch then analyzes the entire dialed string and routes the call based on the administration on the Dial Plan Parameters screen.

Note:

- Non-IP telephones and trunks inherit the location number of the hardware they are connected to (for example, the cabinet, remote office, or media gateway).
- IP telephones indirectly obtain their location number.
    - A location number is administered on the IP Network Region screen that applies to all telephones in that IP region.
    - If a **Location** field is left blank on an IP Network Region screen, an IP telephone derives its location from the cabinet where the CLAN board is that the telephone registered through.
- IP trunks obtain their location from the location of its associated signaling group. Either direct administration (only possible for signaling groups for remote offices), or the ways described for IP telephones, determines the location.

Other options for the dial plan

You can establish a dial plan so that users only need to dial one digit to reach another extension. You can also establish a dial plan that allows users to dial, for example, two digits to reach one extension, and three digits to reach another. This is particularly useful in the hospitality industry, where you want users to be able to simply dial a room number to reach another guest.

If you have Communication Manager 5.0 or later, you can administer dial plans per-location. To access a per-location screen, type change dialplan analysis location n, where n represents the number of a specific location. For details on command options, see online help, or *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

Feature access codes

Feature access codes (FAC) allow users to activate and deactivate features from their telephones. A user who knows the FAC for a feature does not need a programmed button to use the feature. For example, if you tell your users that the FAC for the Last Number Dialed is *33, then users can redial a telephone number by entering the FAC, rather than requiring a Last Number Dialed button. Many features already have factory-set feature access codes. You can use these default codes or you can change them to codes that make more sense to you. However, every FAC must conform to your dial plan and must be unique.

Adding feature access codes

About this task

As your needs change, you might want to add a new set of FAC for your system. Before you can assign a FAC on the **Feature Access Code** screen, it must conform to your dial plan.

In our example, if you want to assign a feature access code of 33 to **Last Number Dialed**, first you need to add a new FAC range to the dial plan.

Complete the following steps to add a FAC range from 30 to 39.

Procedure

1. Go to the administration interface.
2. Enter `change dialplan analysis` or `change dialplan analysis location n`, where n represents the number of a specific location. Press `Enter`.
   The Dial Plan Analysis screen appears.
3. Move the cursor to an empty row.
4. Type `3` in the **Dialed String** column and then tab to the next field.
5. Type `2` in the **Total Length** column and then tab to the next field.
6. Type `fac` in the **Call Type** column.
7. Press `Enter` to save your changes.

Changing feature access codes

About this task

If you try to enter a code that is assigned to a feature, the system warns you of the duplicate code and does not allow you to proceed until you change one of them.

Tip:

To remove a feature access code, delete the existing FAC and leave the field blank.

Let us try an example. If you want to change the feature access code for Call Park to *72 do the following.

Procedure

1. Go to the administration interface.

2. Enter **change feature-access-codes**. Press Enter. The Feature Access Code(FAC) screen appears.
3. Move the cursor to the **Call Park Access Code** field.
4. Type *72 in the **access code** field over the old code.
5. Press Enter to save your changes.

Administering Dial Plan Transparency (DPT)

The Dial Plan Transparency (DTP) feature preserves users' dialing patterns when a media gateway registers with a Survivable Remote Server (Local Survivable Processor), or when a Port Network requests service from a Survivable Core Server (Enterprise Survivable Server). Note that this feature does not provide alternate routing for calls made between Port Networks connected through networks other than IP (for example, ATM or DS1C), and that register to different Survivable Core Servers during a network outage.

Administration of Dial Plan Transparency (DPT) is similar to setting up Inter-Gateway Alternate Routing (IGAR). You must first enable the DPT feature, then set up Network Regions and trunk resources for handling the DPT calls. For Survivable Core Servers, you must also assign Port Networks to communities. The following table show the screens and field used in setting up Dial Plan Transparency:

Screen Name	Purpose	Fields
Feature-Related System Parameters	• Enable the DPT feature for your system. • Indicate the Class of Restriction to use for the Dial Plan Transparency feature.	• Enable Dial Plan Transparency in Survivable Mode • COR to use for DPT
IP Network Region	Administer the DPT feature for Network Regions.	• Incoming LDN Extension • Dial Plan Transparency in Survivable Mode
System Parameters-ESS	Enter the community assignments for each Port Network.	Community

For more information on the Dial Plan Transparency feature, see Dial Plan Transparency in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Controlling the features your users can access

Class of service and class of restriction give you great flexibility with what you allow users to do. If you are in doubt about the potential security risks associated with a particular permission, contact your Avaya technical support representative.

Features and functions

Communication Manager offers a wide range of features and functions. Some of these you can administer differently from one user to the next. For example, you can give one user a certain set of telephone buttons, and the next user a completely different set, depending on what each person needs to get his/her job done. You decide on these things as you administer the telephones for these individuals.

Class of service

Often, groups of users need access to the same sets of Communication Manager features. You can establish several classes of service (COS) definitions that are collections of feature access permissions. Now, a user's telephone set can be granted a set of feature permissions by simply assigning it a COS.

Class of restriction

Class of restriction (COR) is another mechanism for assigning collections of capabilities. COR and COS do not overlap in the access or restrictions they control.

System-wide settings

There are some settings that you enable or disable for the entire system, and these settings effect every user. You might want to look over the various System Parameters screens and decide which settings best meet the needs of your users.

To see a list of the different types of parameters that control your system, type **`display system-parameters`**. Press **Help**. You can change some of these parameters yourself. Type **`change system-parameters`**. Press **Help** to see which types of parameters you can change. In some cases, an Avaya technical support representative is the only person who can make changes, such as to the System-Parameters Customer-Options screen.

Type **`list usage`** to see all the instances of an object, such as an extension or IP address, in your system. This is useful when you attempt to change administration and receive an “in use” error. See *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431, for more information.

Changing system parameters

About this task

You can modify the system parameters that are associated with some of the system features. For example, you can use the system parameters to allow music to play if callers are on hold or to allow trunk-to-trunk transfers on the system.

Generally, Avaya sets your system parameters when your system is installed. However, you can change these parameters as your organization's needs change.

For example, let us say that you are told that the number of rings between each point for new coverage paths should change from 4 to 2 rings. Complete the following steps to change the number of rings.

Procedure

1. Go to the administration interface.
2. Enter `change system-parameters coverage/forwarding`. Press `Enter`.
3. The System Parameters Call Coverage/Call Forwarding screen appears.
4. In the**Local Coverage Subsequent Redirection/CFWD No Answer Interval** field, type `2`.
5. Press `Enter` to save your changes.

   Each telephone in a Call Coverage path now rings twice before the call routes to the next coverage point. The Local Cvg Subsequent Redirection/CFWD No Ans Interval field also controls the number of rings before the call is forwarded when you use Call Forwarding for busy/don't answer calls. This applies only to calls covered or forwarded to local extensions. Use Off-Net to set the number of rings for calls forwarded to public network extensions.

WAN Bandwidth Limits between Network Regions

Bandwidth limits

Using the Communication Manager Call Admission Control: Bandwidth Limitation (CAC-BL) feature, you can specify a VOIP bandwidth limit between any pair of IP network regions, and then deny calls that need to be carried over the WAN link that exceed that bandwidth limit.

Bandwidth limits can be administered in terms of:

- Kbit/sec WAN facilities
- Mbit/sec WAN facilities
- Explicit number of connections
- No limit

Considerations for WAN bandwidth administration

Collect design information

It is highly recommended that you have the following design information before setting the bandwidth limits and mapping the connections:

- Network topology and WAN link infrastructure.
- An understanding of the Committed Information Rate (CIR) for the WAN infrastructure.
- Overlay/design of the Network Regions mapped to the existing topology.
- Codec sets administered in the system.
- Bandwidth is assumed to be full duplex.

Typical bandwidth usage

The following table can be used to help assess how much bandwidth (in Kbits/sec) is used for various types of codecs and packet sizes. The values shown assume a 7 byte L2 WAN header (and are rounded up).

Packet Size	10 ms	20 ms	30 ms	40 ms	50 ms	20 ms6
G.711	102	83	77	74	72	71
G.729	46	27	21	18	16	15
G.723-6.3	NA	NA	19	NA	NA	13
G.723-5.3	NA	NA	18	NA	NA	12

These values, when compared to the actual bandwidth used for 8 byte as well as 10 byte L2 WAN headers are not significantly different. In some cases, the rounded up values shown above are greater than values used for 10 bytes.

The bandwidth usage numbers shown above assume 6 bytes for Multilink Point-to-Point Protocol (MP) or Frame Relay Forum (FRF), 12 Layer 2 (L2) header, and 1 byte for the end-of-frame flag on MP and Frame Relay frames for a total of 7 byte headers only. They do not account for silence suppression or header compression techniques, which might reduce the actual bandwidth. For other types of networks (such as Ethernet or ATM) or for cases where there is a lot of silence suppression or header compression being used, the network might be better modeled by administering the CAC-BL limits in terms of number of connections rather than bandwidth used.

Setting bandwidth limits between directly-connected network regions

Procedure

1. Enter **`change ip-network region <n>`**, where n is the region number you want to administer.
2. Scroll to page 3 of the IP Network Region screen which is titled Inter Network Region Connection Management.
3. In the **codec-set** field, enter the number (1-7) of the codec set to be used between the two regions.
4. In the **Direct WAN** field, enter `y`.
5. In the **WAN-BW-limits** field, enter the number and unit of measure (Calls, Kbits, Mbits, No Limit) that you want to use for bandwidth limitation.
6. Press `Enter` to save your changes.

Administering Treatment for Denied or Invalid Calls

About this task

You can administer your system to reroute denied or invalid calls to an announcement, the attendant, or to another extension.

In this example, we want:

- all outward restricted call attempts to route to an announcement at extension 2040
- all incoming calls that are denied to route to the attendant
- all invalid dialed numbers to route to an announcement at extension 2045

Procedure

1. Enter **`change system-parameters features`**.
   The Feature-Related System Parameters screen appears.
2. In the **Controlled Outward Restriction Intercept Treatment** field, type `announcement`.
   Another blank field appears.
3. In this blank field, type `2040`.

   This is the extension of an announcement you recorded earlier.

4. In the **DID/Tie/ISDN Intercept Treatment** field, type `attd`.

   This allows the attendant to handle incoming calls that have been denied.
5. In the **Invalid Number Dialed Intercept** field, type `announcement`. Another blank field appears.
6. In this blank field, type `2045`.

   This is the extension of an announcement you recorded earlier.
7. Press `Enter` to save your changes.

Music-on-hold

Description

Music-on-Hold automatically provides music to a caller placed on hold. Music lets the caller know that the connection is still active. The system does not provide music to callers in a multiple-party connection who are in queue, on hold, or parked.

For more information on locally-sourced Music-on-Hold, see the Locally Sourced Announcements and Music feature in the *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Locally sourced announcements and music

The Locally Sourced Announcements and Music feature is based on the concept of audio source groups. This feature allows announcement and music sources to be located on any or all of the Voice Announcement with LAN (VAL) boards or on virtual VALs (vVAL) in a media gateway. The VAL or vVAL boards are assigned to an audio group. The audio group is then assigned to an announcement or audio extension as a group sourced location. When an incoming call requires an announcement or Music-on-Hold, the audio source that is closest to the incoming call trunk plays.

Storing audio locally minimizes audio distortion because the audio is located within the same port network or gateway as the caller. Therefore, this feature improves the quality of announcements and music on hold. This feature also reduces resource usage, such as VoIP resources, because the nearest available audio source of an announcement or music is played. Locally Sourced Announcements and Music also provides a backup for audio sources because multiple copies of the audio files are stored in multiple locations. Audio sources are assigned either to an audio group or a Music-on-Hold group.

Audio groups

An audio group is a collection of identical announcement or music recordings stored on one or more VAL or vVAL boards. The audio group can contain announcements and music. The nearest recording to a call plays for that call.

Music-on-hold groups

A Music-on-Hold (MOH) group is a collection of externally connected and continuously playing identical music sources. An example of a Music-on-Hold source is a radio station connected to a media gateway using an analog station port. Multiple Music-on-Hold sources can be used in the same system. Like the audio group, the nearest music source to a call plays for that call.

Music-on-hold sources

As with the Music-on-Hold feature, only one music source is defined for a system or for a tenant partition. However, you can define a music source as a group of Music-on-Hold sources. Therefore, both non-tenant and tenant systems can use the group concept to distribute Music-on-Hold sources throughout a system.

Adding an audio group

Procedure

1. Enter **`add audio-group n`**, where n is the group number you want to assign to this audio group, or next to assign the next available audio group number in the system.
   The system displays the Audio Group screen.
2. In the **Group Name** field, type an identifier name for the group.
3. In the **Audio Source Location** fields, type in the VAL boards or vVAL location designators for each audio source in the audio group.
4. Press `Enter` to save your changes.

Adding a Music-on-Hold group

Procedure

1. Enter **`add moh-analog-group n`**, where n is the Music-on-Hold group number.
   The system displays the MOH Group screen.
2. In the **Group Name** field, type in an identifier name for the Music-on-Hold group.
3. In the **MOH Source Location numbered** fields, type in the Music-on-Hold VAL or vVAL source locations.
4. Press `Enter` to save your changes.

Setting music-on-hold system parameters

About this task

You must administer the Music-on-Hold (MOH) feature at the system level to allow local callers and incoming trunk callers to hear music while on hold.

Note:

If your system uses Tenant Partitioning, follow the instructions in Providing music-on-hold service for multiple tenants instead of the instructions below.

Procedure

1. Enter **`change system-parameters features`**.
   The Feature-Related System Parameters screen appears.
2. In the Music/Tone On Hold field, type `music`.
   The Type field appears.
3. In the **Type** field, enter the type of music source you want to utilize for MOH: an extension (ext), an audio group (group), or a port on a circuit pack (port).
4. In the text field that appears to the right of your **Type** selection, type the extension number, the audio group, or the port address of the music source.
5. In the **Music (or Silence) on Transferred Trunk Calls** field, type `all`.
6. Press `Enter` to save your changes.
7. Now administer a class of restriction with **Hear System Music on Hold** set to y to allow your local users to hear Music-on-Hold.

Providing music-on-hold service for multiple tenants

Before you begin

Before you can administer tenants in your system, **Tenant Partitioning** must be set to y on the System-Parameters Customer-Options screen. This setting is controlled by your license file.

About this task

If you manage the switching system for an entire office building, you might need to provide individualized telephone service for each of the firms who are tenants. You can set up your system so that each tenant can have its own attendant, and can chose to have music or play special announcements while callers are on hold.

The following example illustrates how to administer the system to allow one tenant to play Country music for callers on hold, and another to play Classical music.

Procedure

1. Enter **`change music-sources`**.
2. For Source No 1, enter `music` in the **Type** column.
   A **Type** field appears under the **Source** column.
3. In the **Type** field, enter `port`.
   A blank text field appears.
4. Enter the port number, `01A1001` in this case, in the text field.
5. In the **description** field, enter `Country`.
6. Move to Source 3, and enter music in the *Type* column, `port` in the **Type** field, `01A1003` for the port number, and `Classical` for the **Description**.
7. Press `Enter` to save your changes.
8. Enter **`change tenant 1`**.
   The Tenant screen appears.
9. In the **Tenant Description** field, type `Dentist`.

   This identifies the client in this partition.
10. In the **Attendant Group** field, type the attendant group number.

    Note:

    The attendant group number must also appear in the **Group** field of the Attendant Console screen for this tenant.
11. In the **Music Source** field, type `1`.
    Callers to this tenant will now hear country music while on hold.
12. Press `Enter` to save your changes.
13. To administer the next partition, enter **`change tenant 2`**.
14. Administer this tenant, Insurance Agent, to use Attendant Group 2 and Music Source 3. Be sure to change the Attendant Console screen so that this attendant is in group 2. This tenant’s callers will hear classical music on hold.

Receiving Notification in an Emergency

If one of your users calls an emergency service such as the police or ambulance, someone, perhaps the receptionist, security or the front desk, needs to know who made the call. Thus, when the emergency personnel arrive, they can be directed to the right place. You can set up

Communication Manager to alert the attendant and up to ten other extensions whenever an end-user dials an emergency number. The display on the notified user's telephone shows the name and number of the person who placed the emergency call. The telephones also ring with a siren-type alarm, which users must acknowledge to cancel.

Note:

You must decide if you want one user to be able to acknowledge an alert, or if all users must respond before an alert is cancelled. Verify that the **ARS** field is **y** on the System Parameters Customer-Options (Optional Features) screen.

Also, make sure that the extensions you notify belong to physical digital display telephones. Refer to Telephone Reference on page 653 for a list of telephone types. When you assign crisis alert buttons to the telephones, check the Type field on the Station screen to be sure you are not using a virtual extension.

About this task

In this example, we will set up the system to notify the attendant and the security guards at all 3 entrances when someone dials the emergency number 5555. All three guards must acknowledge the alert before it is silent.

Procedure

1. Type `change ars analysis n`. Press `Enter`. The ARS Digit Analysis Table screen appears.
2. In the **Dialed String** field, type `5555`.

   This is the number that end-users dial to reach emergency services.
3. In the**Total Min** and **Max** fields, type `4`.

   In this example, the user must dial all 4 digits for the call to be treated as an emergency call.
4. In the **Route Pattern** field, type `1`.

   In this example, we use route pattern 1 for local calls.
5. In the **Call Type** field, type `alrt`.

   This identifies the dialed string 5555 as one that activates emergency notification.
6. Press `Enter` to save your changes. Now set up the attendant console to receive emergency notification.
7. Type`change attendant 1`. Press `Enter`.

   The Attendant Console screen appears.
8. In the feature button area, assign a **crss-alert** button.
9. Press `Enter` to save your changes.
10. Assign a **crss-alert** button to each security guard's telephone.

    You cannot assign this button to a soft key.

Finally, we make sure that all security personnel and the attendant will have to acknowledge the alert.

11. Type `change system-parameters crisis-alert`. Press `Enter`.

    The Crisis Alert System Parameters screen appears.

12. Go to the **Every User Responds** field and type `y`.

13. Press `Enter` to save your changes.

Notifying a Digital Pager of an Emergency

You have the option of having your emergency calls go to a digital pager. When someone dials an emergency number (for example, 911), the system sends the extension and location (that originated the emergency call) to the administered pager.

Before you begin

Before you start,

- You need to administer a **crss-alert** button on at least one of the following.
    - Attendant Console (use the **`change attendant`** command)
    - Digital telephone set (use the **`change station`** command)
- The **ARS Digit Analysis** Table must have emergency numbers in the **Call Type** column set to **alrt** (crisis alert).
- You need a digital numeric pager.

Procedure

1. Type `change system-parameters crisis-alert`. Press `Enter`.

   The Crisis Alert System Parameters screen appears.

2. In the **Alert Pager** field, type `y`.

   This allows you to use the Crisis Alert to a Digital Pager feature and causes additional crisis alert administration fields to appear.

3. In the **Originating Extension** field, type a valid unused extension to send the crisis alert message. We will type `7768`.

4. In the **Crisis Alert Code** field, type `911`.

   This is the number used to call the crisis alert pager.

5. In the **Retries** field, type `5`.

   This is the number of additional times the system tries to send out the alert message in case of an unsuccessful attempt.

6. In the **Retry Interval (sec)** field, type `30`.

   This is length of time between retries.

7. In the **Main Number** field, type the number that is to be displayed at the end of the pager message. We will type `303-555-0800`.

8. In the **Pager Number** field, type the number for the pager. We'll type `303-555-9001`.

9. In the **Pin Number** field, type `pp77614567890`.

   This is the PIN number, if required, for the pager. Insert any pause digits (pp) as needed to wait for announcements from the pager service to complete before sending the PIN.

10. In the **DTMF Duration - Tone (msec)** field, type `100`.

    This is the length of time the DTMF tone is heard for each digit.

11. In the **Pause (msec)** field, type `100`.

    This is the length of time between DTMF tones for each digit.

12. Press `Enter` to save your changes.

    Refer to the Crisis Alert feature in Feature Description and Implementation for Communication Manager, 555-245-205, for more detailed information.

Other Useful Settings

There are many settings that control how your system operates and how your users telephones work. Most of these you administer through one of the System Parameters screens. This section describes a few of the items you can enable in your system to help your users work more efficiently. See Feature-Related System Parameters for a more detailed description of the available system settings.

Automatic callback if an extension is busy

You can allow users to request that the system call them back if they call a user whose telephone is busy. For more information, see the Automatic Callback feature in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Automatic hold

You can set a system-wide parameter that allows your users to initiate a call on a second line without putting the first call on Hold. This is called Automatic Hold, and you enable it on the

Feature-Related System Parameters screen. If you do not turn this on, the active call drops when a the user presses the second line button.

Bridging onto a call that has gone to coverage

You can allow users to join (bridge) on to a call that rang at their extension and then went to coverage before they could answer. For more information, see the Temporary Bridged Appearance feature in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Distinctive ringing

You can establish different ringing patterns for different types of calls. For example, you can administer your system so that internal calls ring differently from external calls or priority calls. For more information, see the Distinctive Ringing feature in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Warning when telephones are off-hook

You can administer the system so that if a telephone remains off-hook for a given length of time, Communication Manager sends out a warning. This is particularly useful in hospitals, where the telephone being off-hook might be an indication of trouble with a patient. See “Class of Service” for more information.

Warning users if their calls are redirected

You can warn analog telephone users if they have features active that might redirect calls. For example, if the user has activated send all calls or call forwarding, you can administer the system to play a special dial tone when the user goes off-hook. See Distinctive Ringing in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information.

Controlling the Calls Your Users Can Make and Receive

The Avaya Communication Manager provides several ways for you to restrict the types of calls your users can make, and the features that they can access.

You use class of restriction (COR) to define the types of calls your users can place and receive. Your system might have only a single COR, a COR with no restrictions, or as many CORs as necessary to effect the desired restrictions.

You will see the **COR** field in many different places throughout Communication Manager when administering telephones, trunks, agent logins, and data modules, to name a few. You must enter a COR on these screens, although you control the level of restriction the COR provides.

Strategies for assigning CORs

The best strategy is to make it as simple as possible for you and your staff to know which COR to assign when administering your system. You can create a unique COR for each type of user or facility, for example, call center agents, account executives, administrative assistants, Wide Area Telecommunications Service (WATS) trunks, paging zones or data modules.

You can also create a unique COR for each type of restriction, for example, toll restriction, or outward restriction. If you have a number of people who help you administer your system, using this method would also require the additional step of explaining where you wanted to use each type of restriction.

Note:

COR-to-COR calling restrictions from a station to a trunk do not apply when Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), or Uniform Dial Plan (UDP) is used to place the call. In these cases, use Facility Restriction Levels to block groups of users from accessing specific trunk groups. See Class of Restriction and Facility Restriction Levels in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information.

To find out what CORs are administered in your system already, type `list cor`. You can also display information for a single COR by typing list `cor #`.

Allowing users to change CORs

You can allow specific users to change their Class of Restriction (COR) from their telephones using a Change COR feature access code. You can also limit this feature by insisting that the user enter a password as well as a feature access code before they can change their COR. The Station Lock feature also allows users to change their own COR.

Insert an optional short description to be used as link preview or summary text. See the shortdesc tag help for a more detailed description of appropriate usage of shortdesc.

Before you begin

Before you start:

- Be sure that **Change COR by FAC** field is set to `y` on the System-Parameters Customer-Options (Optional Features) screen. Note that you cannot have both **Change COR by FAC** and **Tenant Partitioning** enabled.
- Be sure that each user (who you want to allow to change a COR) has a class of service with console permissions.

About this task

To allow users to change their own class of restriction, you must define a feature access code and can, optionally, create a password. For example, we will create a change COR feature access code of *55 and a password of 12344321.

Procedure

1. Type `change feature-access-codes`. Press `Enter`.

   TheFeature Access Code (FAC) screen appears.
2. Move the cursor to the **Change COR Access Code** field.
3. Type `*55` in the **access code** field.
4. Press `Enter` to save your changes.

   Now we have to define the password.
5. Type `change system-parameters features`. Press `Enter`.

   The Feature-Related System Parameters screen appears.
6. Press `Next Page` to find the Automatic Exclusion Parameters section.
7. Move to the **Password to Change COR by FAC** field and enter `12344321`.

   This field determines whether or not Communication Manager requires the user to enter a password when they try to change their COR. Avaya recommends that you require a password.
8. Press `Enter` to save your changes.

Station Lock

Station Lock provides users with the capability to manually lock their stations, using a button or feature access code, in order to prevent unauthorized external calls from being placed.

Station Lock can prevent unauthorized external calls. Telephones can be remotely locked and unlocked. Station Lock allows users to:

- Change their Class of Restriction (COR); usually the lock COR is set to fewer calling permissions than the station's usual COR
- Lock their telephones to prevent unauthorized outgoing calls.
- Block outgoing calls and still receive incoming calls.
- Block all outgoing calls except for emergency calls.

Station Lock is activated by pressing a telephone button, which lights the button indicator, or by dialing a FAC.

Analog and XMOBILE stations must dial a FAC to activate the feature. The user hears a special dial tone on subsequent origination attempts from the telephone to indicate that the lock feature is active.

Digital stations including DCP, BRI, IP hardphones and softphones access Station Lock with a feature button or through a FAC. H.323 or DCP phones support the station lock functionality of Communication Manager. SIP phones do not support the functionality. The Station Lock feature is activated in the following cases:

- If a digital or IP telephone has a feature button for Station Lock but uses a FAC to activate the feature, the LED lights up. The system generates the special tone.
- If a digital or IP telephone has a feature button for Station Lock and uses this button to activate the feature, the LED lights up. The system generates the special tone.
- If a digital or IP telephone does not have a feature button for Station Lock and uses a FAC to activate the feature, the system generates the special tone.

A station can be locked or unlocked from any other station if the FAC is used and the Station Security Code is known. The attendant console can never be locked but can be used to lock or unlock other stations. A station also can be locked or unlocked via a remote access trunk.

Interactions

- Attendant Console

  Station Lock cannot be used for attendant consoles but it can be assigned to regular digital stations that might also have console permissions. The FAC cannot be used to activate Station Lock for the attendant console, but the FAC can be dialed from the attendant console in an attempt to remotely activate or deactivate Station Lock for another station.

- Personal Station Access (PSA)

  Station Lock can be used for PSA stations as long as they are associated with an extension. When stations are disassociated, Station Lock cannot be activated.

- Remote Access

  After a remote user dials a valid barrier code, the user receives system dial tone. To activate/deactivate Station Lock, the user must dial the FAC, then the extension number, then the security code number.

Station Lock by time of day

Beginning with Communication Manager 4.0 or later, you can you can also lock stations using a Time of Day (TOD) schedule.

To engage the TOD station lock/unlock you do not have to dial the station lock/unlock FAC, or use **stn-lock** button push.

When the TOD feature activates the automatic station lock, the station uses the Class of Restriction (COR) assigned to the station lock feature for call processing. The COR used is the same as it is for manual station locks.

The TOD lock/unlock feature does not update displays automatically, because the system would have to scan through all stations to find the ones to update.

The TOD Station Lock feature works as follows:

- If the station is equipped with a display, the display will show “Time of Day Station Locked”, if the station invokes a transaction which is denied by the Station Lock COR. Whenever the station is within a TOD Lock interval, the user will hear a special dial tone instead of the normal dial tone, if the special dial tone is administered.
- For analog stations or without a display, the user hears a special dial tone. The special dial tone has to be administered and the user hears it when the station is off hook.

After a station is locked by TOD, it can be unlocked from any other station if the Feature Access Code (FAC) or button is used. You have to also know the Station Security Code, and that the **Manual-unlock allowed?** field on the Time of Day Station Lock Table screen is set to `y`.

Once a station has been unlocked during a TOD lock interval, the station remains unlocked until next station lock interval becomes effective.

If the station was locked by TOD and by Manual Lock, an unlock procedure will unlock the Manual Lock as well as the TOD Lock (“Manual-unlock allowed?” field on the Time of Day Station Lock Table screen is set to `y`).

The TOD feature does not unlock a manually locked station.

Note:

The attendant console cannot be locked by TOD or manual station lock.

Screens for administering Station Lock

Screen name	Purpose	Fields
COR	Administer a Class of Restriction (COR) that allows the user to activate Station Lock with a feature access code (FAC).	**Station Lock COR**
Feature Access Code (FAC)	Assign one FAC for Station Lock activation, and another FAC for Station Lock Deactivation.	**Station Lock Activation** Station Lock Deactivation
Station	Assign the user a COR that allows the user to activate Station Lock with an FAC.	**COR** **Time of Day Lock Table**

Screen name	Purpose	Fields
	Assign a sta-lock feature button for a user.	Any available button field in the **BUTTON ASSIGNMENTS** area
	Assign a Station Security Code (SSC) for a user.	**Security Code**
Time of Day Station Lock Table	Administer station lock by time of day.	**Table Active** **Manual Unlock Allowed** **Time Intervals**
Feature Related System Parameters	Enable special dial tone.	**Special Dial Tone**

Chapter 4: Administering Communication Manager on Avaya S8xxx Servers

This chapter describes how to administer Communication Manager on Avaya S8xxx Servers. It is targeted for system administrators after the product is installed and tested. In a converged network where voice and data are both sent over a corporate local area network (LAN), this configuration can provide primary or standby telephony and communications-processing capabilities.

Users should have broad data networking experience with data products and technology to best understand this product. An in-depth knowledge of the call-processing engine of Communication Manager.

Overview of administering Avaya servers

To set up and maintain your Avaya S8xxx Server with an H.248 Media Gateway, you need to administer:

- the Media Gateway and its internal processors, typically using a command-line interface (CLI)
- the Avaya S8xxx Server using the Server Web Interface
- call-processing features using Communication Manager

H.248 Media Gateway administration

For details on any hardware components, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

For details on any media gateways, see the following:

- *Administration for the Avaya G250 and Avaya G350 Media Gateways*, 03-300436
- *Administration for the Avaya G430 Media Gateway*, 03-603228
- *Administration for the Avaya G450 Media Gateway*, 03-602055

Survivable Remote Servers configuration

An Avaya S8xxx Server can be configured either as the primary call-processing controller, or as a Survivable Remote Server (Local Survivable Processor). A Survivable Remote Server can take over call processing if the primary call-processing system (such as another Avaya server) is unavailable for any reason (such as a network failure or server problem). The Avaya S8xxx Server can be either the primary or Survivable Remote Server; it is set up to operate as a primary or standby Survivable Remote Server during the configuration process using the Server Web Interface. The license file determines the mode that the server runs in and the Configure Server Web page provides supplementary instruction.

If the Avaya S8xxx Server loses contact with its Media Gateway, the media gateway retains its last status until the Link Loss Delay Timer (LLDT) expires. (The default for the LLDT is 5 minutes, but this interval is administrable using the **Link Loss Delay Timer (minutes)** field on the IP-Options System Parameters screen. Once the LLDT expires, the system removes all boards and deletes all call processing information. However, if the Media Gateway loses contact with the Avaya S8xxx Server, the media gateway first tries to reconnect for a period of one minute. If this fails, the Media Gateway tries to connect with another server in its controller list. If the primary server was a Survivable Remote Server, it will start looking at the top of its MGC list in order to get back to the primary server. Otherwise, it starts down the list of alternative servers. When a functional Avaya S8xxx Server is located, the media gateway informs the server of its current call state, and the server maintains those connections until the users hang up.

If the primary call-processing server goes offline and a Survivable Remote Server is available as a standby unit, it will assume call processing as follows:

- IP telephones and media gateways that were previously using the primary server will try to register with the standby server for call processing, provided that they have been administered to do so in the controller list (use the `set mgc list` command).
- The standby server (Survivable Remote Server) will go into license error mode, then start to provide call processing. It cannot preserve any calls set up by the primary server. IP telephone connections can stay up until the call is completed if they are shuffled, but no features are supported on the call.

  Note:

  The license error mode runs for up to 30 days, and if the problem is not resolved, the system goes into No License Mode and administration and some commands are restricted.
- If the standby server is rebooted, all devices will return to using the primary server for call-processing service. Any calls in progress on the Survivable Remote Server will be

dropped when the reboot occurs (the change back to the primary server is not call preserving).

- With Survivable Remote Server functionality, there is full functionality and feature support.

Command line interface administration

Instead of using Device Manager, you can access the server’s command line interface using Telnet and an IP address of 192.11.13.6.

- Command line interface (CLI) access procedures are covered in *Welcome to the Avaya G700 Media Gateway controlled by an Avaya S8300 Media Server or an Avaya S8700 Media Server*, 555-234-200.
- For a list of CLI commands, see the *Maintenance for the Avaya G700 Media Gateway controlled by an Avaya S8300 Media Server or an Avaya S8700 Media Server*, 555-234-101.

SNMP alarms are different from server hardware- or software-generated Operations Support System (OSS) alarms that are recorded in the server logs, and might be reported through SNMP notifications. Alarms generated by Communication Manager and System Platform are managed through the Secure Access Link (SAL) remote architecture. Either method, both, or no alarm-reporting method might be used at a given site.

Avaya S8xxx Server administration

You can install a Communication Manager template on a Avaya S8xxx Server to control its operation over the corporate network. Some of the primary functions controlled by the Avaya S8xxx Server are:

- Backing up and restoring call processing, server, and security data using the System Management Interface.
- Checking server and process status.
- Monitoring the health of the system.
- Updating and managing patches.
- Installing license and authentication files.
- Managing security configuration for the server.
- Installing new software and reconfiguring the server as needed.
- Performing System and Alarm configuration.

- Rebooting or shutting down the server.
- Managing users and passwords.

Access and administer Communication Manager

You can access and administer Communication Manager in the following ways:

- Starting a SAT session
- Accessing the System Management Interface
- Accessing the System Platform Web Console
- Logging on to the System Manager web interface

Starting a SAT session

Before you begin

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable the IP forwarding feature.

Procedure

1. Enter the unique IP address of the Avaya S8xxx server. For example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server as `craft` or `dadmin`.
3. Suppress alarm origination.

Access System Management Interface

Accessing the System Management Interface

About this task

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a laptop connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a laptop connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, System Management Interface supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address of the Avaya S8xxx Server in standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a DNS server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

   - Laptop access by IP address

     If you log on to the services port from a directly connected laptop, the IP address must be the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other Avaya S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   ✱ **Note:**

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Accessing the Server Administration Interface

About this task

The Server Administration Interface allows you to maintain, troubleshoot, and configure the Avaya S8xxx Server.

Procedure

From the Communication Manager SMI home page, on the **Administration** menu, click **Server (Maintenance)**.

The tasks you can perform are shown by a list of links in the panel on the left side of the screen.

For help with any of these tasks, click **Help** on this home page. Click **Help** on any of the pages accessed by the links to go directly to the help for that specific screen.

Server Administration Interface tasks

Key tasks that administrators typically perform on Avaya S8xxx Servers are summarized in this section. See online help for more detailed information.

File copying to the server

Files must be copied to the Avaya S8xxx Server from another computer or server in the network, or uploaded from a directly connected laptop computer. Files that might be copied to the server include license and authentication files, system announcements, and files for software upgrades. Files can be copied to the server using one of the following methods:

- Upload Files to Server (via browser) link to upload one or more files from your computer to the server's FTP directory using HTTP protocol.
- Download Files to Server (from Web) link to copy files to the server from another server on the network; it works like the Upload Files screen.
- Transfer files from another computer or server accessible from the corporate network using FTP or Trivial FTP (TFTP). Files must be transferred in binary mode. Either a GUI or CLI FTP program can be used, depending on what is available on your computer.

Error resistant download through https

Communication Manager provides a more robust system upgrade experience.

After a Communication Manager upgrades, the system:

- Reduces copy size from files size (which currently can approach 100MB) to something more granular (for example: block size) such that when remote upgrades are being performed over a bouncing network, much of the copying is done without re-transmittal.
- Supports SCP and HTTPS protocols to allow secure file transfers.
- Views the progress of the upgrade file transfers and processes, specifically that the process is progressing and not hung. The progress is displayed in text only format.

SNMP setup

You can set up Simple Network Management Protocol (SNMP) services on the server to provide a means for a corporate NMS to monitor the server, and send alarm notifications to a services agency, to a corporate NMS, or both. For more information on administering SNMP, see SNMP Administration.

To activate SNMP alarm notification for devices, use the SNMP Traps screen to set up SNMP destinations in the corporate NMS. SNMP traps for other devices on the network can be administered using Device Manager. See Device Manager administration for Media Gateway components.

Note:

UDP port 162 for snmptrap must be “opened” to allow reception of traps (from media gateways) and transmission of traps to your trap receiver. Certain trap categories from media gateways must be administered “on” by media gateway administration. Use media gateway commands **`set snmp trap enable auth`** and **`tcp syn-cookies`** for this. For more information on media gateways, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431 and *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300432.

System Platform Web Console overview

The System Platform Web interface is called System Platform Web Console. After installing System Platform, you can log on to the System Platform Web Console to view details of System Platform virtual machines (namely, System Domain (Dom-0) and Console Domain), install the required solution template, and perform various administrative activities by accessing options from the navigation pane.

In the navigation pane, the system lists the administrative options under three categories: Virtual Machine Management, Server Management, and User Administration.

Virtual Machine Management

Use the options under Virtual Machine Management to view details and manage the virtual machines on System Platform. Some of the management activities that you can perform include rebooting or shutting down a virtual machine.

The System Domain (Dom-0), Console Domain, and components of the solution templates running on the System Platform are known as virtual machines. The System Domain (Dom-0) runs the virtualization engine and has no direct management access. Console Domain (cdom or udom) provides management access to the system through the System Platform Web Console.

Server Management

Use the options under Server Management to perform various administrative activities for the System Platform server. Some of the administrative activities that you can perform include:

- Configuring various settings for the server
- Viewing log files
- Upgrading to a latest release of the software
- Backing up and restoring current version of the software

User Administration

Use the options under User Administration to manage user accounts for System Platform. Some of the management activities that you can perform include:

- Viewing existing user accounts for System Platform
- Creating new user accounts
- Modifying existing user accounts
- Changing passwords for existing user accounts

Accessing the System Platform Web Console

Before you begin

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 11.

About this task

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.

4. Click **Continue**.

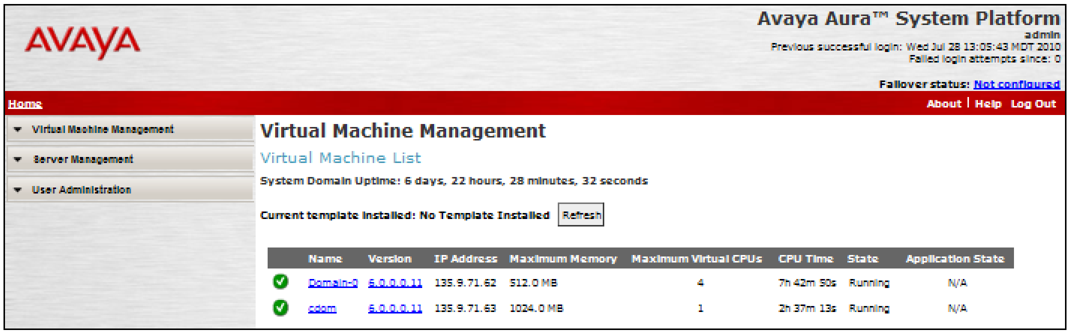
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Related topics:

Enabling IP forwarding to access System Platform through the services port on page 11

System Platform backup

You can back up configuration information for System Platform and the solution template (all virtual machines). Sets of data are backed up and combined into a larger backup archive. Backup sets are related data items that need to be backed up. When you perform a back up, the system executes all the backup sets. All the backup sets must succeed to produce a backup archive. If any of the backup sets fail, then the system removes the backup archive. The amount of data backed up is dependent on the specific solution template.

The system stores the backup data in the `/vspdata/backup` directory in Console Domain. This is a default location. During an upgrade, the system does not upgrade the `/vspdata` folder, so that you can restore the data, if required. You can change this location and back up the System Platform backup archives to a different directory in System Platform or in an external server. You can also send the backup data to an external e-mail address if the file size is not larger than 10 MB.

If a backup fails, the system automatically redirects you to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup is successful.

Note:

It is not the aim of the backup feature to provide a mechanism to re-enable a failed High Availability Failover node back to High Availability Failover configuration. Follow the instructions in this document on how to re-enable failed High Availability Failover node back to High Availability Failover configuration.

For configuring System Platform backup, see *Administering Avaya Aura™ System Platform*.

Avaya Aura System Manager overview

System Manager is a central management system that delivers a set of shared management services and a common console for System Manager and its components. System Manager includes the following shared management services:

Service	Description
Elements	Provides you features offered by individual components of System Manager. Except some links that provide access to generic features provided by System Manager, most of the links provides access to features provided by different components of System Manager.

Service	Description
Events	Provides you features for administering alarms and logs generated by System Manager and other components of System Manager. You can view and change the status of alarms. For logs, you can view logs, harvest logs for System Manager and its components, and manage loggers and appender.
Groups & Roles	Provides you features for administering groups and roles. You can create and manage groups, roles, and permissions.
Licenses	Provides you features for administering licenses for individual components of Avaya Aura Unified Communication System.
Routing	Provides you features for managing routing applications. You can create and manage routing applications that includes Domains, Adaptations, SIP Entities, Entity Links, Time Ranges, Policies, Dial Patterns, and Regular Expressions to configure your network configuration.
Security	Provides you the features for configuring certificates
System Manager Data	Provides you features for: • Backing up and restoring System Manager configuration data. • Monitoring and scheduling jobs. • Replicating data from remote nodes. • Configuring data retention settings and profile for various services provided by System Manager.
Users	Provides you the features to administer users, shared address, public contact list and system presence access control list information. You can create and manage user profiles. You can associate the user profiles with groups, roles, communication profiles, create a contact list, add address, and private contacts for the user.

Logging on to the System Manager Web interface

The System Manager Web interface is the main interface of Avaya Aura™ System Manager. You must log on to the System Manager Web console before you can perform any tasks.

Before you begin

A user account to log on to the System Manager Web interface. If you do not have a user account, contact your system administrator to create your account.

Procedure

1. On the browser, type the Avaya Aura™ System Manager URL (`https://<SERVER_NAME>/SMGR`) and press the **Enter** key.
2. In the **Username** field, enter the user name.

3. In the **Password** field, enter the password.
4. Click **Log On**.

   If your user name and password:

   - Match an authorized System Manager user account, System Manager displays the Avaya Aura™ System Manager Home page with the Avaya Aura™ System Manager Version *version_number*. The System Manager home page displays navigation menu in the left navigation pane. The menu provides access to shared services using which you can perform various operations supported by System Manager. The tasks you can perform depends on your user role.

     The content page in the right pane displays shortcut links that provides access to the shared services.
   - If you enter incorrect login credentials in theSystem Manager login page, System Manager displays an error message, and prompts you to re-enter the user name and password so that you can log in again.

System Manager- Communication Manager capabilities overview

System Manager provides a common, central administration of some of the existing IP Telephony products. With System Manager, you can consolidate the key capabilities of the current suite of Integrated Management administration products with other Avaya Management tools on a common software platform. System Manager helps you administer Avaya Aura™ Communication Manager, Communication Manager Messaging, and Modular Messaging. The capabilities of System Manager include:

- Endpoint management
- Template management
- Mailbox management
- Discovery management
- Element Cut Through to native administration screens

Managing Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. System Manager also allows you to directly add, edit, view or delete these objects through **Communication Manager**.

Endpoint management

System Manager allows you to create and manage endpoints. Endpoint management provides support for Communication Manager endpoint objects and helps you add, change, delete, and view endpoint data.

Templates

Using templates, you can specify specific parameters of an endpoint or a subscriber once and then reuse that template for subsequent add endpoint or subscriber tasks. The system provides default templates, but additionally you can also add your own custom templates.

There are two categories of templates: default templates and user-defined templates. You cannot edit or delete the default templates. However, you can modify or remove user-defined templates any time.

Subscriber management

System Manager lets you manage subscriber data. Subscriber management provides support for Communication Manager Messaging and Modular Messaging objects. You can add, change, remove, and view subscriber data.

Using System Manager Communication Manager capabilities, you can:

- Add Communication Manager for endpoints and Modular Messaging for subscribers to the list of managed elements.
- Create templates to simplify endpoint and subscriber management.
- Administer endpoints, subscribers, and create user profiles with Communication Profiles.
- Associate the user profiles with the required endpoints and subscribers.

Main and Survivable Remote split registration prevention administration

Split registrations occur when resources in one network region are registered to different servers. For example, after an outage activates Survivable Remote Servers (Local Survivable Processors), telephones in a network region register to the main server, or Survivable Core Server (Enterprise Survivable Server), while the gateways are registered on the Survivable Remote Server. The telephones registered with the main server are isolated from their trunk and VOIP resources.

The split registration prevention solution enables the administrator to manage system behavior after an outage. The administrator can force telephones and gateways to register with the main server or the Survivable Remote Server.

Detailed description of Main and Survivable Remote split registration prevention

Avaya provides the following alternatives for managing split registration prevention:

- Set the **Migrate H.248 MG to primary** field on the System Parameters Media Gateway Automatic Recovery Rule screen to `immediately`.
- Use the feature described in this section.

It handles split registrations occurring between a main server and Survivable Remote Servers or between a Survivable Core Server and Survivable Remote Servers. This solution does not handle split registration between a main server and a Survivable Core Server.

When aggregation at the main server or Survivable Core Server is preferred, all the telephones and media gateways register with the main server or Survivable Core Server.

When aggregation at the Survivable Remote Server is preferred, the main server or Survivable Core Server disables the network regions associated with the Survivable Remote Server, forcing all the telephones and gateways in the regions to register with the Survivable Remote Server. Re-registration to the main server or Survivable Core Server is not allowed till one of the following conditions is satisfied:

- The time-day-window for automatic return to the main server is reached for at least one of the media gateways in any of the regions the Survivable Remote Server is backing up.
- The **`enable mg-return`** command is executed. After re-registration to the main server or Survivable Core Server starts, it continues until the Survivable Remote Server reports inactive status, one hour elapses since execution of the **`enable mg-return`** command, or until you run the **`disable mg-return`** command.
- The Survivable Remote Server unregisters from the main server or Survivable Core Server.

Split registration prevention solution

The main server (Communication Manager) attempts to ensure that the devices in a network region register to the same server. They can register either with the Survivable Remote Server or the main server. When administered or set, telephones and gateways can be forced to register with active Survivable Remote Servers. The split registration prevention solution keeps branch-oriented operations intact with local trunk and VOIP resources.

Survivable Remote Servers report as active after a media gateway registers itself. The main server does not allow any further re-registration of media gateways and telephones already registered with the Survivable Remote Servers.

Split registration prevention solution sequence of events

The administrator enables the split registration prevention solution. The main server resets or the network fragments, causing a media gateway to unregister.

The following sequence of events occur:

1. The media gateway registers to a Survivable Remote Server.
2. The Survivable Remote Server reports its active status to the main server.
3. The main server unregisters all media gateways and telephones in the regions backed up by the Survivable Remote Server.
4. The main server enables the endpoints in those regions to re-register upon the arrival of the day and time specified in the time-day-window or until the **`enable mg-return`** command is executed.

Network design notes for split registration prevention solution

These notes and network design recommendations apply while administering the split registration prevention solution:

- The **`disable nr-registration`** [**`disable network region registration`**] is executed in a region having media gateways. A Survivable Remote Server becomes active when a media gateway registers itself to it. The main server disables all regions backed up by the Survivable Remote Server.

  The execution of **`enable nr-registration`** [**`enable network region registration`**] in a region puts a region to auto disable (**`ad`**) if the Survivable Remote Server backing the region is active. All other regions backed up by that Survivable Remote Server are left in auto disabled state.
- The command, **`enable nr-registration`** has no effect to enable a region which is automatically disabled by the split registration prevention feature.
- A Survivable Core Server allows Survivable Remote Servers to register when the administrator sets **Force Phones and Gateways to Active LSPs** to `y`.
- All media gateways should have trunks and VoIP resources. If H.248 media gateways without those resources are the only ones registered to a Survivable Remote Server, the Survivable Remote Server accepts telephone registrations but the telephones cannot make trunk calls. This event is similar to the situation when G650 media gateways without those resources are the only port networks controlled by a Survivable Core Server.
- Split registrations between the main server and Survivable Core Server may occur if the Survivable Core Server's processor Ethernet addresses are included in any Telephone Alternate Gatekeeper Lists (AGLs) or Media Gateway Controller lists (MGC). Administrators can include C-LANs controlled by Survivable Core Server in AGLs. If a

Telephone registers to a C-LAN controlled by a Survivable Core Server, it can use trunks on the same G650 port network holding the C-LAN.

- When administering the media gateway's MGC list, the part of the list below the Survivable Remote Server transition point must contain only one entry administered under the Media Gateway region's BACKUP SERVERS heading on the IP Network Region screen.
- Communication Manager main servers do not allow a Survivable Remote Server entry under the column heading BACKUP SERVERS IN PRIORITY ORDER to be changed if the corresponding Survivable Remote Server is currently registered and active.
- All media gateways in a single network region using time-day-window media recovery rules should follow the same rule. Communication Manager handles any violation to this recommendation well. Any variation to the recovery rules creates confusion about further events.
- The Alternate Gatekeeper List that is provided to IP telephones after they reboot should contain the Survivable Remote Server's address at the end of the list. If the Survivable Remote Server's address is not in the list at all, and if the main server is unreachable after a power failure, the telephones cannot reach the corresponding Survivable Remote Server.

Network region type description

A Survivable Remote Server is administered as a backup server for one or more network regions. The Survivable Remote Server can have resources from one or more network regions. When the Survivable Remote Server reports its active status to the main server, the network regions' statuses change to auto disable (**`ad`**). On reaching the time-day-window for automatic return to the main server or executing the **`enable mg-return`** command, the network regions are automatically enabled and the telephones and media gateways can register.

Execute the **`status nr-region`** command to display the status of all the network regions and media gateways in those regions.

On executing the **`disable nr-registration`** command, the network region status changes to manually disabled (**`rd`**). The administrator changes this status by executing the **`enable nr-registration`** command.

When a Survivable Remote Server reports active to the main server, if any of the regions that Survivable Remote Server is a backup server for were manually disabled on the main server, the main server changes those regions' status to auto disable (ad).

For more information on the **`status nr-region`** command, see status nr-registration in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

Split registration prevention solution implementation procedures

This section describes the procedures to implement the split registration prevention solution.

Split registration prevention solution prerequisites and constraints

The main server, Survivable Remote Server, and Survivable Core Server must be running on Communication Manager Release 5.2 or later.

If Survivable Core Servers run Communication Manager Release 5.2 but the main server runs an older version, the split registration prevention solution is disabled.

For administering the split registration prevention solution, the following conditions must be met:

- You can set the **Migrate H.248 MG to primary** field on the Systems Parameters Media Gateway Automatic Recovery Rule screen to `time-day-window`. You can also set this field to other rules when no other media gateways are using the rules.
- The BACKUP SERVERS IN PRIORITY ORDER column in the IP Network Region screen must have only a single Survivable Remote Server entry. The number of non-Survivable Remote Server entries in this column is not affected. After implementing the split registration prevention solution, only one Survivable Remote Server entry is allowed under BACKUP SERVERS IN PRIORITY ORDER.

Enforcing the split registration prevention solution

Procedure

1. Enter `change system-parameters ip-options`.
2. Press `Enter` until you see the **Force Phones and gateways to Active LSPs** field.
3. To enable the solution, set the **Force Phones and gateways to Active LSPs** field to `y`.

   The default value for the field is set to `n`.
4. Select `Enter` to save your changes.

   Note:

   You can set **Force Phones and gateways to Active LSPs** to `y` if all administered mg-recovery-rules are set to time-day-window. At most, one Survivable Remote Server is listed as a Backup Server for each ip-network-region.

Disabling the split registration prevention solution

Procedure

1. Enter `change system-parameters ip-options`.
2. Press `Enter` until you see the **Force Phones and gateways to Active LSPs** field.
3. To disable the solution, set the **Force Phones and gateways to Active LSPs** field to `n`.
4. Select `Enter` to save your changes.

   ✱ **Note:**

   You can set **Force Phones and gateways to Active LSPs** to **`n`** only if all registered Survivable Remote Servers are inactive.

Return to the main server

If one Media Gateway returns to the main server meeting any of the conditions for re-registration, all regions backed up by the same Survivable Remote Server also return to the main server.

Gateways and Endpoints can return to the main server if the Survivable Remote Server unregisters from the main Communication Manager server.

Return to main server continues at least until one of these events occurs.

- The Survivable Remote Server administered under the region's BACKUP SERVERS heading on IP Network Region screen becomes inactive.
- Expiry of the current one hour interval in the time-day-window that makes the first media gateway eligible to re-register.
- One hour has elapsed since the **`enable mg-return`** command was run or earlier if during that hour the system administrator runs the **`disable mg-return`** command.

Administrable Alternate Gatekeeper List for IP Phones

Communication Manager enables the Alternate Gatekeeper List (AGL) feature to allow administrators to specify the number of IP interfaces for each connected network region that are allowed for telephones within a specific network region.

The Administrable Alternate Gatekeeper List feature limits the number of entries in the AGL, and is intended to simplify network region administration. This feature can improve system performance and reliability. It also reduces the time that it takes for telephones to failover to the Survivable Core or Survivable Remote Server.

This feature enhancement is available to all H.323 telephone types, and does not require any Communication Manager license file feature activation or firmware upgrades.

The H.323 telephones use the Alternate Gatekeeper List (AGL) when they cannot reach or register with their primary gatekeeper. H.323 telephones use the AGL list of C-LANs/PE for recovery when the current C-LAN is no longer available. The Survivable Remote Servers may be a separate failover set if the alternatives for reaching the main server are exhausted.

H.323 telephones can receive from the Communication Manager server an AGL with up to 6 Survivable Remote Servers and 1 survivable gateway. This is true whether or not the phones' region is using the Administrable AGL feature. Without AGL, the number of non-survivable IP interface addresses in the network region depends on several factors:

- If the current Ethernet interface is a C-LAN with TN799c vintage 3 or older firmware, the ordinary gatekeeper part of the list is truncated at 15 entries.
- If the telephone is not Time-to-Service (TTS) capable, the ordinary gatekeeper part of the list is truncated at 30 entries, but 46xx telephones with non-SW hardware must be used with up to 28 entries.
- If the telephones is TTS capable, the ordinary gatekeeper part of the list is truncated at 65 entries.

You can continue to use the AGL feature of prior releases (up to 65 C-LAN or PE members in the AGL). Alternately, you can choose to use the more efficient method of controlling telephone recovery by condensing the number of gatekeepers sent by Communication Manager based on new network region administration.

To use the Communication Manager AGL feature, administrators enter a numeric value in the **AGL** field of the Inter Network Region Connection Management screen. Use the Inter Network Region Connection Management screen to administer connections between a source network region and all other destination network regions. The entries administered in the **AGL** field within each source network region represent the number of C-LANS and/or PE that Communication Manager builds into each Alternate Gatekeeper List and sends to each H.323 telephone that is in that source network region. After entering the numeric values, Communication Manager calculates the total number of gatekeepers that are assigned for each destination region. The total AGL assignments for each region must add up to 16 or lower. If an administrator enters a value that makes the AGL assignment greater than 16, the system displays an error message.

Communication Manager tracks each C-LAN or PE addresses sent in the AGL to each telephone. For example, a destination network region with 20 C-LANs are administered to have only 3 C-LANs from that region in each AGL. As a result, Communication Manager responds to each new registration request with an AGL constructed using the administered number of C-LANs for the region, and is independent of priority, socket load, and service state.

Note:

If Communication Manager is upgrading to a newer version, the pre-upgrade AGL lists are not disturbed unless the administrator makes any changes to the **AGL** fields and enters new values.

For more information on the administration procedures for this feature, see Administrable Alternate Gatekeeper List administration.

Load balancing of IP telephones during registration

Non-TTS telephones are load balanced at registration using the Gatekeeper Confirm (GCF) message. Each region has a list of available C-LANs or PE, and Communication Manager selects the most available C-LAN within the IP (H.323) telephone's home network region. If there are C-LANs in that network region, the system uses load balancing techniques based on C-LAN priority, and available sockets. If all C-LANs are considered busy (none of the C-LANs are in service, or all C-LANS that are in service have used all the 480 available sockets), Communication Manager moves to directly connected network regions. All directly connected regions are checked beginning with network region 1. All indirect network regions are used if there were no C-LANs administered in the IP telephone's home network region, or directly connected network regions. Indirect network regions are also checked by the system beginning with network region 1.

With the enhanced implementation of the feature in Communication Manager 5.1 for load balancing for non-TTS telephones, the system gives preference to the home region C-LANs, then the direct network region C-LANs, followed by indirect network region C-LANs that are administered using the new **AGL** field on the Inter Network Region Connection Management screen. Any C-LAN within an eligible region may be assigned for load balancing. Within a specific region, the system selects the least loaded C-LAN, unless all C-LANs have reached their limit.

Load balancing for non-TTS telephones is based on the C-LAN received in gatekeeper confirm (GCF). Non-TTS phones use this C-LAN to initiate the registration request (RRQ) as well as establish a socket to Communication Manager after Registration Admission Status (RAS) has been completed.

Socket load balancing for TTS telephones occurs after registration is complete and the AGL has been formed. Communication Manager initiates socket establishment to TTS phones. Load balancing occurs across the C-LANs that were sent in the AGL, with preference being given to the C-LANs in the home region, then the directly connected regions, followed by the indirectly connected regions. Direct network regions and indirect network region C-LANs are considered as two groups. The system checks for the most available C-LAN in directly connected network regions, followed by the available C-LAN in indirectly connected network regions. Communication Manager determines that a preferred set of C-LANs is at their limit before attempting to access the next set of C-LANs.

When sending the gatekeeper list with the administrable AGL feature, the system uses each network region (home, direct, indirect) and sends a subset of the C-LANs starting at a random place in the C-LAN array.

How Alternate Gatekeeper Lists are built

Communication Manager 5.1 builds the AGL for each telephone during registration using the following parameters:

- Communication Manager builds the AGL based on the C-LANs for the home region. For non-TTS and TTS telephones, the AGL is built using a random starting point in the network region C-LAN array. Communication Manager picks the administered number of C-LANs from that initial point, based on the number of C-LANs administered in the **AGL** field of the Inter Network Region Connection Management screen.
- The system then continues building the AGL based on the list of administered directly connected regions. The order of regions is selected by round robin method, and the C-LANs are selected based on the same random algorithm that is used for selecting C-LANs from the home region.
- The system continues building the AGL for indirectly connected regions in the same way as it does for directly connected network regions.

The difference in the Communication Manager 5.1 enhancement of this feature is that the IP (H.323) telephone can now use C-LANs from all network regions as alternate gatekeepers, as long as they are connected (directly or indirectly) to the native region. The alternate gatekeepers are sent in the following order: in-region, directly connected regions, and indirectly connected regions.

Contact your Avaya representative if you have additional questions relating to how Communication Manager 5.1 builds the Alternate Gatekeeper Lists.

Applications for AGL

This section describes two common issues that are addressed by the Administrable Alternate Gatekeeper List feature for Communication Manager.

The examples are based on configurations using WAN facilities. In both examples, a virtual network region is assigned to the WAN to describe the WAN topology, and to implement Call Admission Control (CAC).

- Example 1 shows how you can ensure that the IP telephone does not receive unwanted C-LANs in the Alternate Gatekeeper List. It also shows the improved configuration for this issue.
- Example 2 shows how pooling C-LANs in a network region results in some IP telephones not receiving an Alternate Gatekeeper List. It also shows the improved configuration for this issue.

Prevent unwanted C-LANs in the AGL example

This example shows how you can ensure that the IP telephone does not receive unwanted C-LANs in the Alternate Gatekeeper List. It also shows the improved configuration for this issue.

The figure on page 72 shows how unwanted C-LANs can end up in the Alternate Gatekeeper List.

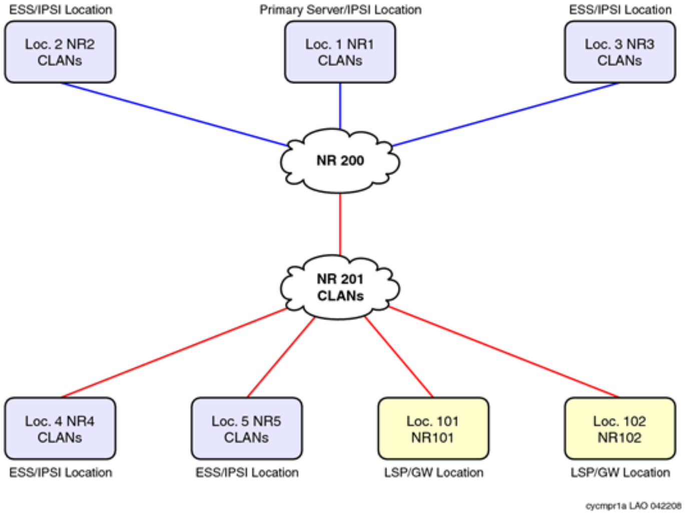


Figure 1: Unwanted C-LANs in Pre-Communication Manager 5.1 AGL

In this configuration, the IP telephones in NR1 through NR3 have C-LANs in their network regions as there are no C-LANs that are directly connected to NR200. You can optionally add a few C-LANs in NR200 to share with NR1-NR3 as they are directly connected, and NR 200 is used to consolidate traffic from NR1-NR3 for access to the WAN. Using NR 200 has the additional advantage of isolating C-LANS in each network region to IP telephones in that network region.

NR4 and NR5 are Survivable Core Server locations, and the IP telephones in those two locations need local C-LANs that are in NR4 and NR5.

NR101 and NR102 are Gateway/Survivable Remote Server locations and should share pooled C-LANS. In this case, C-LANS are placed in NR201 as it is directly connected to the two NRs. Before Communication Manager 5.1 C-LANs could be in home region of the IP Phone, or in a directly connected NR.

The IP telephones in NR4 and NR5 receive C-LANs in NR201 in the AGL as that NR is directly connected. The IP telephones can end up with C-LANS in their AGL that cannot be used in a WAN failure. This can significantly delay IP telephones in NR4 and NR5 from recovering to a C-LAN that can be used in a WAN failure. This could also significantly delay IP telephones in NR4 and NR5 from recovering to a Survivable Core Server.

The figure on page 73 shows a pre-Communication Manager 5.1 workaround that you can implement using another virtual network region.

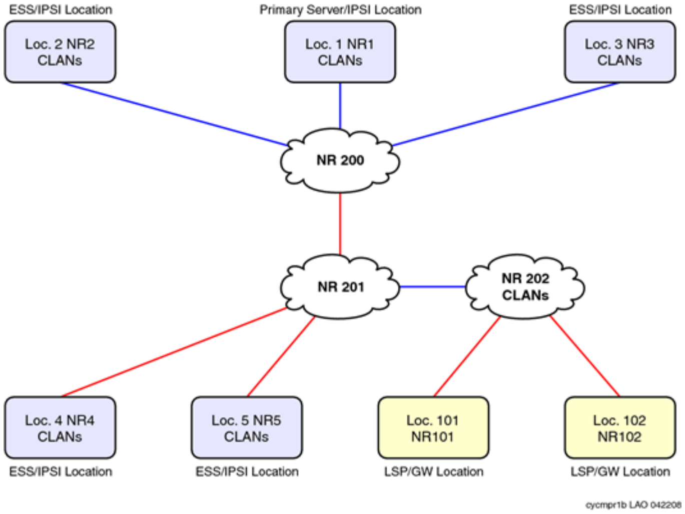


Figure 2: Pre-CM5.1 workaround for unwanted C-LANs

In this configuration, the IP telephones in NR4 and NR5 use the ip-network-map for NR assignment. The AGL does not contain NR202 C-LANs because that NR is indirectly connected.

The IP telephones in NR101 and NR102 share C-LANs in NR202. Those C-LANs are physically located at location 1. If there are a large number of C-LANs in NR202, it could result in large AGLs and potentially delay recovery to the Survivable Core Server. This workaround does not address the size of the AGL.

The figure on page 74 shows the improved configuration of the network region using the Administrable AGL feature for Communication Manager 5.1.

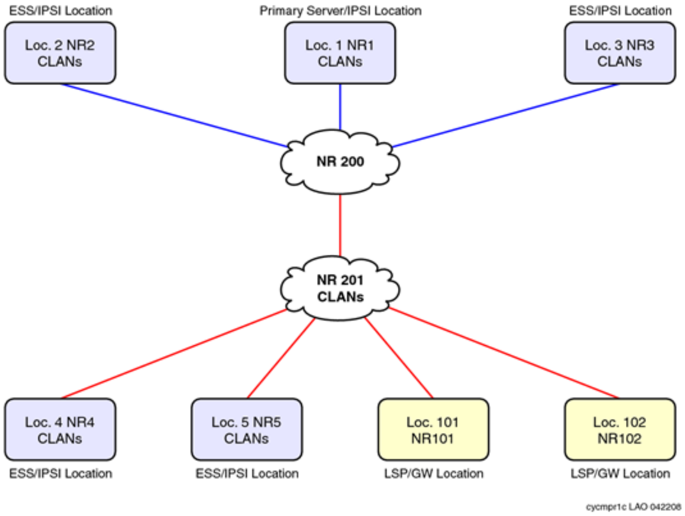


Figure 3: Improved configuration for unwanted C-LANs using the enhanced AGL feature

The figure on page 74 shows a configuration in which the IP telephones in NR4 and NR5 are administered to only use C-LANS in their native NR, and not use C-LANs in NR201. The IP telephones AGLs in NR4 and NR5 contain local C-LANs. The IP telephones in NR101 and NR102 share C-LANs in NR201. Those C-LANS are physically located at location 1. If there are a large number of C-LANs in NR201, it could result in large AGLs and potentially delay recovery to the Survivable Core Server.

Additionally, with this enhancement, the administrator can specify the number of C-LANs in NR201 and therefore control the size of the AGL.

Pool C-LANS despite Network Region Connectivity issues example

This example shows how pooling C-LANs in a network region results in some IP telephones not receiving an Alternate Gatekeeper List. It also shows the improved configuration for this issue.

The figure on page 75 shows how network region connectivity issues can prevent the pooling of C-LANs.

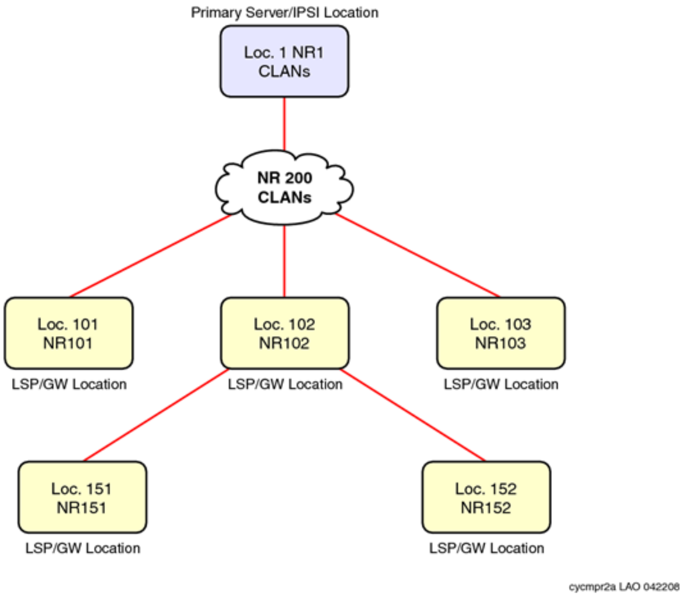


Figure 4: Inadequate pooling of C-LANs

The figure shows a network configuration with numerous Gateway/Survivable Remote Server locations, some of which are directly connected to the WAN, and others that are indirectly connected to the WAN. All of these gateways need to share a pool of C-LANS physically located at location 1.

The IP telephones in NR151 and NR152 are not directly connected to NR200. Also, the system cannot specify the number of C-LANs in NR200 to use to control size of AGL.

The figure on page 76 shows the workaround that you can use in the pre-Communication Manager 5.1 implementation.

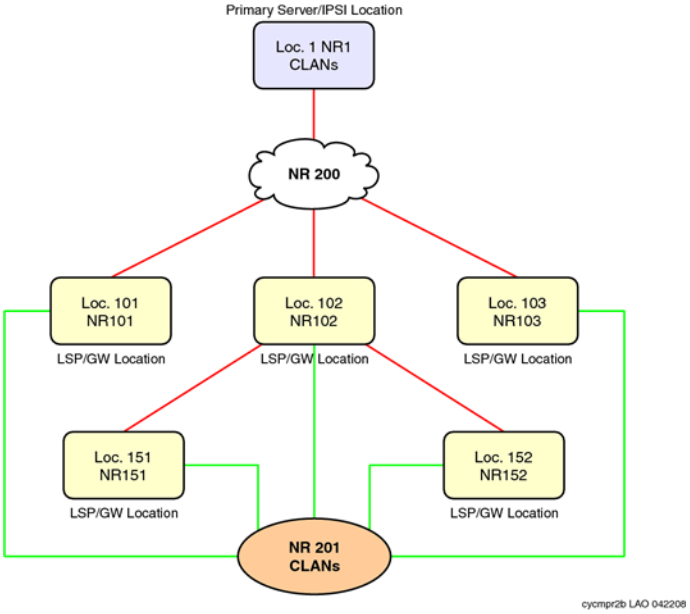


Figure 5: Pre-CM5.1 workaround for inadequate pooling of C-LANs

In this configuration, all the IP telephone network regions are directly connected to a new NR201. The AGL now contains C-LANs in NR201. But you cannot specify number of C-LANs in NR201 that you can use to control size of AGL. This configuration does not reflect the WAN topology.

The figure on page 76 shows the improved configuration using the Communication Manager 5.1 Administrable AGL feature.

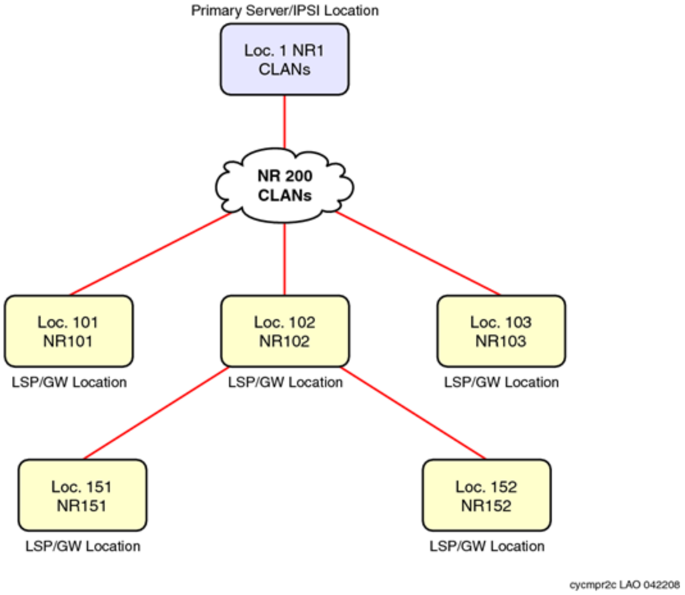


Figure 6: Improved configuration using the CM5.1 AGL feature

All IP telephones AGL contain C-LANs in NR200, including the direct and indirect network regions. You can also specify the number of C-LANs in NR200 and control the size of the AGL.

AGL high-level capacities

The total AGL assignments for each source region must sum to 16 or lower. Each source network region can continue to have 6 Survivable Remote Servers from the phone's home region to be added to the AGL. This brings the total list size to a maximum of 23 (by adding up the AGL, Survivable Remote Server for each region and the Survivable Gatekeeper for the station).

Considerations

If the telephone's IP address is not in one of the ranges in the ip-network-map, the AGL entries consist of the C-LANs/PE from the telephone's homed region only. Note that administering an phone's ip-address in a network map allows the associated AGL to work more robustly by accessing directly and indirectly connected regions, as well as the homed region.

Interactions

This section provides information about how the Administrable AGL feature for Communication Manager 5.1 interacts with other features on the system.

- It is possible to have some regions using the pre-Communication Manager 5.1 non-administrable AGL implementation, and some other regions using the new administrable AGL implementation. But you cannot have a single network region using a combination of the two methods. The AGL column can either contain numbers or all, but not both. The field can also contain blanks; blanks are ignored by both the old and the new implementation of this feature.
- This feature only applies to H.323 IP telephone registrations and H.323 IP telephone AGLs. The H.323 gateways also register to Communication Manager. This feature does not affect how the gateways obtain and use their own lists of gatekeepers. Also note that this feature has no impact on how IP (SIP) telephones register to SM 6.0 or SES 5.2 and earlier.
- If an extension number has shared control using the server between an IP (H.323) telephone and an IP (H.323) softphone, Communication Manager displays both the AGL that was sent to the H.323 telephone and the AGL that was sent to the H.323 softphone.
- In prior releases of Communication Manager, the AGL feature only included C-LANs from the same region and from directly connected regions, or all indirectly connected regions (if there were no C-LANS in the same or directly connected regions). With this

enhancement, it is now possible to explicitly administer Communication Manager to include C-LANs from indirectly connected regions as well. Also, if you administer a non-zero value in the AGL column for an indirectly connected region, it opens that indirectly connected region's C-LANs to be eligible to be used for load balancing.

- In general, when using the Communication Manager 5.1 Administrable AGL feature, C-LAN priorities should not be used. Note the following additional information:
    - For TTS telephones, the Communication Manager 5.1 enhanced feature takes into consideration priorities and C-LAN socket load, as well as C-LAN’s service state and whether the C-LANs are allowed to be used for H.323 IP telephone registration when load balancing.
    - For non-TTS phones, priorities and C-LAN socket load are taken into account when load balancing.
    - For TTS and non-TTS telephones, the Communication Manager 5.1 enhanced feature does not take either priorities or C-LAN socket load into consideration when building the AGL.

Administrable Alternate Gatekeeper List administration

Use the following procedures to administer the Communication Manager Administrable Alternate Gatekeeper List feature on your system:

Preparing to administer Alternate Gatekeeper Lists

Procedure

1. Verify that your system is running Communication Manager Release 5.1 or later
2. Complete basic administration procedures for H.323 telephones

Configuring Administrable Alternate Gatekeeper Lists

Procedure

1. Enter `change ip-network-region` **`x`**, where **`x`** is the number of the network region that you want to administer.

   The system displays the Inter Network Region Connection Management screen. Page down till you see the page with the AGL column.
2. Check your settings for the AGL column.

a. To use the Administrable Alternate Gatekeeper List feature, you have to enter a numeric value in that field for the region that you want to administer.

   You can enter the values from `0` through `16`. This value determines how many C-LAN addresses from that destination region are included in the Alternate Gatekeeper List when a telephone registers in the source region.

   Note:

   The system enables you to use the Communication Manager administrable AGL option only if every row has a numeric value, or is blank. Communication Manager ignores blank values.

b. If the value is **`all`** or blank, the system uses the Communication Manager Release 5.0 or earlier version of this feature to determine alternate gatekeeper lists.

c. If the value is **`all`** for any row(s), you cannot enter a number into any of the other rows.

   In this case, you have to set them to **`all`** or blank. Note that if the value for every row is **`all`** or blank, the system automatically uses the Communication Manager Release 5.1 or earlier method for using AGL.

3. Select `Enter` to save your changes.

Viewing IP Network Maps for your system

Procedure

1. Enter `change ip-network-map`.
2. The fields on this screen display the IP addresses of each region and the phones they are mapped to.
3. View your network maps.
4. Select **Enter** to save your changes and exit the screen.

Verifying AGL settings for stations

Procedure

1. Enter `status station` **`XXXXX`** where **`XXXXX`** is the extension of the station registered to the region having a numeric value for its AGL, which means it is using the Administrable AGL feature.
2. Page down till you find the page for the Alternate Gatekeeper List.

3. This screen shows the AGL mappings with the IP interfaces listed in order.

   The screen also shows the network region of each IP interface entry in the AGL.

   The fields shown on this screen are display only. See the descriptions of the IP Network Region Screen and the Station Screen in the *Avaya Aura™ Communication Manager Screen Reference*, 03-602878 for related information.
4. View the information for your system.
5. Select `Enter` to exit the screen.

Troubleshooting scenarios and repair actions for AGL

The Station screen (command: **`status station`**) can sometimes show a different AGL than the telephone is actually using under these circumstances.

- If you change the region that a telephone registers to by changing the ip-network-map, Communication Manager does not download the new AGL to that telephone until you re-register the telephone.
- The **`status station`** command shows what the system sent to the telephone. The system does not know what the telephone actually stores. If the system sends an AGL to a telephone and the telephone reboots after that, the AGL that the telephone got from the Dynamic Host Configuration Protocol (DHCP) server can differ from the one displayed by the **`status station`** command.
- If the gatekeeper sending the RCF to the telephone is not in the AGL, some telephones add that gatekeeper's address to the telephone's own local copy of the AGL.

Related Documents for AGL

See the following documents at http://www.avaya.com/support

- *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504
- *Avaya Aura™ Communication Manager Screen Reference*, 03-602878
- *Avaya Application Solutions: IP Telephony Deployment Guide*, 555-245-600
- *Avaya Aura™ Communication Manager Survivable Options*, 03-603633
- *Application Notes for Administrable Alternate Gatekeeper List for IP Phones Using Communication Manager*, Issue 1.0
- *Communication Manager Network Region Configuration Guide for Communication Manager 3.0*

Improved Port network recovery from control network outages

When network fail, IP connected port networks experience disproportionately long outages from short network disruptions. This feature enables you to see IP connected port networks with less downtime in the face of IP network failures.

When there is a network outage, port networks do a warm restart rather than a reset to allow faster recovery of service.

The feature lessens the impact of network failures by:

- Improving TCP recovery times that increase the IPSI-PCD socket bounce coverage time from the current 6-8 seconds range for the actual network outage to something closer to 10 seconds. Results vary based on traffic rates.
- Modifying the PKTINT recovery action after a network outage to entail a warm interrupt rather than a PKTINT application reset (hardware interrupt)). This prevents H.323 IP telephones from having to re-register and/or have their sockets regenerated. This minimizes recovery time from network outages in the range of 15-60 seconds.

This feature also monitors the IPSI-PCD socket and helps in identifying and troubleshooting network related problems.

The IPSI-PCD socket bounce is developed by improving TCP recovery time that covers typical network outages, up to a range of 10-11 seconds. In this scenario, uplink and downlink messages are buffered, and operations very quickly return to normal after a network failure. In order to improve recovery time for longer outages, up to the 60 seconds range, the feature introduces the use of a PKTINT warm interrupt rather than a reset. This results in less drastic action being taken to recover links and H.323 IP telephones.

During the network outage, only stable calls already in progress have their bearer connections preserved. A stable call is a call for which the talk path between the parties in the call is established. Call control is not available during the network outage, and this means that any call in a changing state is most likely not preserved.

Some examples are:

- Calls with dial tone
- Calls in dialing stage
- Calls in ringing stage
- Calls transitioning to/from announcements
- Calls transitioning to/from music-on-hold
- Calls on hold

- Calls in ACD queues
- Calls in vector processing

Further, you cannot change in the state of a preserved call. So, features such as conference or transfer are not available on the preserved calls. Button pushes are not recognized. Invocation of a feature by the user is given denial treatment. In a conference call, if a party in the call drops, the entire call is dropped.

The following are additional improvements:

- Improve TCP Recovery Time
- Increase IPSI Local Buffering to prevent data loss
- Reduce escalation impact between 15 and 60 seconds by using warm interrupt of PKTINT instead of PKTINT application reset (hardware interrupt).
- Reduce escalation impact between 60 and 90 seconds by extending PN cold reset action from 60 seconds to 90 seconds
- Reduce Survivable Core Server No Service Timer minimum value from 3 minutes to 2 minutes to reduce local outage in case of prolonged network outage
- List measurements for the PCD-PKTINT socket for improved troubleshooting

With the introduction of a warm interrupt of the PKTINT instead of reset in the 15-60 seconds range, and the optional extension of the PN cold reset from 60 to 120 seconds.

For more information on System parameters screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Network recovery configuration impacts on availability

Communication Manager reduces the downtime experienced by port networks after a short network outage. In Communication Manager Release 5.2, the H.323 endpoint and application link, and the socket stability are improved in the sub-60 second range than Communication Manager Release 5.1 and earlier. H.323 endpoints using TTS do not have to regenerate sockets, and H.323 endpoints not using TTS do not have to re-register or regenerate their sockets.

Improved survivability administration

Reducing the minimum Survivable Core Server No Service Time Out Interval from 3 to 2 minutes improves overall availability.

Call-processing Administration

The telephony features of the S8300D Server are administered using the same commands and procedures as an S8700-Series Server or a legacy DEFINITY Enterprise Communications System.

Communication Manager Access

Communication Manager resides on the Avaya S8xxx Server. It can be accessed through Avaya Site Administration (ASA), the System Access Terminal (SAT) program, or the Native Configuration Manager interface.

AvayaSiteAdministration

Avaya Site Administration features a graphical user interface (GUI) that provides access to SAT commands as well as wizard-like screens that provide simplified administration for frequently used features. You can perform most of your day-to-day administration tasks from this interface such as adding or removing users and telephony devices. You can also schedule tasks to run at a non-peak usage time.

Note:

In order for ASA to work properly with the ASG Guard II, the **Write (ms)** field on the **Advanced** tab of the Connection Properties screen must be set to a value of 5 (that is, delay of 5 ms). ASG Guard II is an outboard appliance providing access security for Avaya products that do not have Access Security Gateway (ASG) software as a native application. For more information on ASG Guard II, contact your Avaya technical support representative.

For more information, see Using Avaya Site Administration in System Basics.

System Access Terminal

The System Access Terminal (SAT) program uses a Command Line Interface (CLI) interface for telephony administration. SAT is available through the Avaya Site Administration package.

Security Considerations

Levels of security for administration of the Media Gateway are the same as traditionally for Communication Manager. This means that administration login passwords are passed in plain text with no encryption. Exceptions to this no-encryption policy include:

- The ASG program that is installed on all Avaya S8xxx Servers.
- An encrypted Web interface to the Avaya S8xxx Server (see the security certificate information in the server online help).
- Optional encryption for data backups (see Data backup and restore).
- Support for RADIUS authentication for media gateways.

Command syntax changes for media modules

The syntax for using the SAT commands for a Media Gateway or Avaya S8xxx Server has changed. In a traditional DEFINITY system, ports are identified by the cabinet number, carrier, slot, and port. For example: 02A0704

Because this numbering convention does not make sense for media modules, a new convention was developed. The numbering convention for the media modules uses the same seven-character field as does a traditional system, but the fields represent the media gateway number, media module slot (V1 to V9), and port number (00 to 99 are supported; the actual number of ports that can be specified depends on the type of media module).

Example: 001V205

In this example, the 001 represents the media gateway number, the V2 represents the slot number (possibly V1 through V9), and 05 is the port number.

Communication Manager SAT CLI access

You can access the command line interface (CLI) of the Communication Manager SAT using any of the following methods:

- Secure Shell remote login
- Using Telnet over The Customer LAN
- Accessing the Native Configuration Manager
- Configuring Avaya Site Administration

Secure Shell remote login

You can log in remotely to the following platforms using Secure Shell (SSH), a secure protocol:

- G250, G350, G430, G450, and G700 Media Gateways
- S8300D, S8510, and S8800 Servers Linux command line
- Communication Manager System Administration Terminal (SAT) interface on an Avaya S8XXX Server using port 5022.

The SSH capability provides a highly secure method for remote access. The capability also allows a system administrator to disable Telnet when it is not needed, making for a more secure system.

Note:

The client device for remote login must also be enabled and configured for SSH. Refer to your client P.C. documentation for instructions on the proper commands for SSH.

Enabling SSH or SFTP sessions on the C-LAN or VAL circuit packs

About this task

Prerequisites:

- TN799BP (C-LAN) with Release 3.0 firmware.
- VAL with Release 3.0 firmware.
- Communication Manager Release 3.0 or later

Procedure

1. Enter `enable filexfr [board location]`.
2. Enter a 3-6 alphabetic character login in the **Login** field.
3. Enter a 7-11 character password (one character must be a number) in the first **Password** field.
4. Renter the same password in the second **Password** field.
5. Set the **Secure?** field to `y`.
6. Select `Enter`.

   SFTP is enabled on the circuit pack, and the login/password are valid for 5 minutes.

Disabling SFTP sessions on the C-LAN or VAL circuit packs

Procedure

1. Enter `disable filexfr [board location]`
   SFTP is disabled on the circuit pack.
2. Select `Enter`

Using Telnet over the Customer LAN

About this task

Note:

For ease of administration, it is recommended that, whenever possible, you use the Avaya Terminal Emulator, or access the server's command line interface using an SSH client, like PuTTY, and an IP address of 192.11.13.6., instead of Telnet.

Procedure

1. Make sure you have an active Ethernet (LAN) connection from your computer to the Avaya S8xxx Server.
2. Access the telnet program; for example:
   - On a Windows system, go to the **Start** menu and select **Run**.
   - Enter `telnet <server_IP_address> 5023`. You might also type the server name if your company's DNS server has been administered with the Avaya S8xxx Server name.
3. When the **`login`** prompt appears, enter the appropriate user name (such as *cust* or *craft*).
4. When prompted, enter the appropriate password or ASG challenge.
5. If you log in as **`craft`**, you are prompted to suppress alarm origination.
   Generally you should accept the default value (yes).
6. Enter your preferred terminal type.

Enabling transmission over IP networks for TTY and fax calls example

Before you begin

The endpoints sending and receiving calls must be connected to a private network that uses H.323 trunking or LAN connections between gateways and/or port networks. Calls must be able to either be passed over the public network using ISDN-PRI trunks or passed over an H.323 private network to Communication Manager switches that are similarly enabled.

Therefore, you must assign the IP codec you define in this procedure to the network gateways. For our example, the network region 1 will be assigned codec set 1, which you are enabling to handle fax and TTY calls.

Procedure

1. Enter `change ip-codec-set 1`.
2. Complete the fields as required for each media type you want to enable.
3. Select **Enter** to save your changes.

   For more information on fax/TTY over IP, see *Avaya Aura™ Communication Manager Administering Network Connectivity on* , 555-233-504.

Accessing the Native Configuration Manager

About this task

The Server Administration Interface allows you to administer the Avaya S8xxx server using a graphically enhanced SAT applet.

Procedure

1. From the Communication Manager SMI home page, on the **Administration** menu, click **Native Configuration Manager**.

   ⚠ **Warning:**

   Closing this window while the Native Configuration Manager applet is running, exits the applet without displaying a warning.

   After successful installation of the applet, the system displays the Server Login window.
2. In the **Logon** field, type your user name.
3. The system displays the Remote host authentication window. You must authenticate the host.
4. In the **Password** field, type your password. Click **OK**.

   After successful authentication, the system displays the Native Configuration Manager home page.

Logging in to the Avaya S8xxx Server with ASA

Procedure

1. To start Avaya Site Administration, click **Start** > **Programs** > **Avaya** > **Site Administration** .

   Avaya Site Administration supports a terminal emulation mode, which is directly equivalent to SAT command interface. Avaya Site Administration also supports a whole range of other features, including the GEDI and Data Import. For more information refer to the Online Help, Guided Tour, and Show Me accessed from the Avaya Site Administration Help menu.
2. To use Avaya Site Administration, open the application and select the Avaya S8xxx Server you want to access. When prompted, log in.
3. When you are logged in, click **Start GEDI**.

Administration screen and command summary

The following screens are used to administer Media Gateways, Avaya S8xxx Servers, and other media modules.

Communication Manager commands to administer Media Gateways

Communication Manager SAT commands and screens to administer media gateways include:

The Media-Gateway administration screen is used to administer Media Gateways and their media modules. Information is similar to the list media-gateway screen (next item), but also includes MAC address, network region, location and site data.

Note:

For more information about the Media-Gateway screen, and a description of commands, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

- The **`list media-gateway ['print' or 'schedule']`** command shows the list of currently administered gateways. Information includes the media gateway number, name, serial number, IP address, and whether or not this media gateway is currently registered with the call controller. The IP address field is blank until the media gateway registers once, then remains populated.

- The **`list configuration media-gateway x`** command allows you to list all the assigned ports on the media modules for the Media Gateway specified by its number (**`x`**).

System-Parameters Customer-Options (Optional Features) screen

For a complete description of the System Parameters Customer-Options (Optional Features) screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

- The OPTIONAL FEATURES section contains a **Local Survivable Processor** field. If it displays a y (yes), this Avaya S8xxx Server is configured to provide standby call processing in case the primary server is unavailable. See Local Survivable Processor configuration on page 52 for details.

  For information on how to set the display-only field, see Licensing of Communication Manager in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

- Two additional fields in this section indicate if the primary call-processing controller is an S8300D Server. If traditional port networking is disabled and Processor Ethernet is enabled, an S8300D Server is controlling telecommunications.

  - **Port Network Support**: set to **`n`** indicates that traditional port networking is disabled. An S8300D Server is the primary call controller.
  - **Processor Ethernet:** set to **`y`** indicates the presence of an S8300D Server.

Quality of Service Monitoring screens

Several screen changes allow you to monitor Quality of Service (QoS) on an Avaya S8xxx Server with a Media Gateway configuration. The media gateway can send data to a real-time control protocol (RTCP) server, which in turn monitors the network region's performance. Screens include:

- An RTCP MONITOR SERVER section on the IP-Options System Parameters screen allows you to enter a single default IP address, server port, and RTCP report period that can be utilized by all administered network regions. This means you do not have to re-enter the IP address each time you access the IP Network Region screen.
- The IP Network Region screen also must be administered for QoS monitoring (for details, see *Avaya Aura™ Communication Manager Administering Network Connectivity on*, 555-233-504). If the **RTCP Enabled** field is left at default (y), then be sure to set a valid IP address in the IP-Options System Parameters screen. For situations that require

customization, this screen is administered on a per IP network regional basis. Items to customize include:

  - Enabling or disabling of RTCP monitoring
  - Modifications to the report flow rate
  - Changes to the server IP address and server port

- The **`list ip-network-region qos, list ip-network-region monitor`** and **`list ip-network-region igar-dpt`** commands list quality of service and monitor server parameters from the IP Network Region screen as follows:

  - **qos** displays VoIP media and call control (and their 802.1p priority values), BBE DiffServ PHB values, RSVP profile and refresh rate.
  - **monitor** displays RTCP monitor server IP address, port number, report flowrate, codec set, and UDP port range parameters.
  - **`igar-dpt`** displays output for the regions which have administered either of the below fields.

    i. Incoming LDN Extension

    ii. Maximum Number of Trunks to Use for IGAR

    iii. Dial Plan Transparency in Survivable Mode set to “y”.

  - **`list ip-network-region igar-dpt`** command gives an overview of IGAR/DPT-related fields to developers and field support personnel that do not have quick access to ASA.

Media Gateway serviceability commands

Additional commands related to media gateways appear in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431. These include:

- The **`status media-gateways`** command provides an alarm summary, busyout summary, and link summary of all configured media gateways.
- Several commands have been modified to support the media gateway port identification format described in Command syntax changes for media modules. These include:

  - Message Sequence Trace (mst)
  - display errors
  - display alarms

Voice or Network Statistics administration

In Communication Manager Release 5.2, the Voice or Network Statistics feature provides voice and network related measurement data through the SAT interface to help you troubleshoot voice quality issues. The media processor board collects various data elements. The three elements that are used to generate the voice quality measurement reports are **Packet Loss**, **Jitter**, and **RT Delay**.

Note:

The voice or network statistics feature supports only TN2302/TN2602 media processor boards.

You can administer the thresholds of these **Packet Loss**, **Jitter**, and **RT Delay** data elements. The media processor starts collecting the data when any one of these administered thresholds are exceeded for a call. If you change any of the thresholds in the middle of a measurement hour the new values is sent to the board on a near real-time basis. You must set the thresholds high to avoid reporting events when the users are not experiencing voice quality issues.

Before generating voice or network statistics reports, you must specify the network region and the corresponding media processor board on the Network Region Measurement Selection and on the **Media Processor Measurement Selection** screens respectively. Otherwise the system displays the `not a measured resource` error message.

You can set the **Enable Voice/Network Stats** field to `y` on the System Parameters IP Options screen to enable the measurement of voice or network statistics at a system wide level. You can set the **Enable VoIP/Network Thresholds** field to `y` on the IP Interface screen to enable the recording at a single media processor board level. If the **Enable VoIP/Network Thresholds** field set to y, their corresponding default value **Packet Loss**, **Jitter** , and **RT Delay** fields appears on the IP Interface screen.

If you change the **Enable Voice/Network Stats** field from `n` to `y`, the system checks the compatibility of the installed media processor boards and checks if the board is specified on the Media Processor Measurement Selection screen. If the media processor board is not a valid TN2302/TN2602 board, the system displays the `Board must be a valid TN2302 or TN2602` error message.

If you change the **Enable Voice/Network Stats** field from `y` to `n`, the system checks to ensure that the board is removed from the Media Processor Measurement Selection screen. If the media processor board is not removed, the system displays the `This board(s) will automatically be removed from the meas-selection media-processor form` warning message. If you press enter again, the media processor board is removed from the Media Processor Measurement Selection screen.

Note:

Before measuring the voice or network statistics for up to 50 boards, you must administer media processor boards on the Circuit Packs screen, IP Interface screen and Measurement Selection screen. To avoid having to go back and forth between the IP Interface screen and the Media Processor Measurement Selection screen for each media processor board, it is recommended that you administer all boards for which you want to collect data on the Media Processor Measurement Selection screen.

You can generate the report to record the voice statistics for each of the threshold criteria and for the data calls at both an hourly and summary level. You can view this report at both a network region and media processor board level. Report reflects data for up to 24 hours period. You can generate the following reports:

- Hourly Jitter Network Region report – The Hourly Jitter Network Region report assess the jitter at the network region per hour during calls.
- Hourly Delay Network Region report – The Hourly Delay Network Region report assess the round trip delay at the network region per hour during calls.
- Hourly Packet Loss Network Region report – The Hourly Packet Loss Network Region report assess the packet loss at the network region per hour during calls.
- Hourly Data Network Region report – The Hourly Data Network Region report assess the data calls which exceeded a threshold event at the network region. This report is not applied to the specific threshold exceeded, but applies only to pass-through and TTY relay calls, which exceed any one of the three thresholds.
- Hourly Jitter Media Processor report – The Hourly Jitter Media Processor report assess the jitter at the media processor region per hour during calls.
- Hourly Delay Media Processor report – The Hourly Delay Media Processor report assess the round trip delay at the media processor region per hour during calls.
- Hourly Packet Loss Media Processor report – The Hourly Packet Loss Media Processor report assess the packet loss at the media processor region per hour during calls.
- Hourly Data Media Processor report – The Hourly Data Media Processor report assess the data calls which exceeded a threshold event at the media processor region. This report is not applied to the specific threshold exceeded, but applies only to pass-through and TTY relay calls which exceed any one of the three thresholds.
- Summary Jitter report – The summary jitter report summarizes up to five worst jitter calls for the corresponding peak hour for a given media processor board in the network region.
- Summary Round Trip Delay report – The summary round trip delay report summarizes up to five worst round trip delay calls for the corresponding peak hour for a given media processor board in the network region.
- Summary Packet Loss report – The summary packet loss report summarizes up to five worst packet loss calls for the corresponding peak hour for a given media processor board in the network region.
- Summary Data report – The summary data report summarizes up to five worst data calls for the corresponding peak hour for a given media processor board in the network region.

You can also view a near real time voice statistics on the Status Station screen that includes any threshold exception data gathered during a call in progress.

For more information on the voice or network statistics reports, refer to *Avaya Aura™ Communication ManagerReports*, 555-233-505.

SNMP Administration

The SNMP protocol provides a simple set of operations that allow devices in a network to be managed remotely. Communication Manager 4.0 and later releases supports the following versions of SNMP:

- SNMP Version 1 (SNMP v1) and SNMP Version 2c (SNMP v2c): SNMP v1 was the initial version of SNMP. Security in SNMP v1 and SNMP v2c is based on plan-text strings known as communities. Communities are passwords that allow any SNMP-based application to gain access to a device's management information.
- SNMP Version 3 (SNMP v3): SNMP v3 provides additional security with authentication and private communication between managed entities.

The server's Server Administration Interface is used to perform the following functions for SNMP:

- Administer an SNMP trap: For more information, see SNMP traps administration.
- Administer an SNMP agent: For more information, see SNMP agents administration.
- Administer a filter: For more information, see SNMP filters administration.
- View the G3-Avaya-MIB: For more information, see SNMP agents administration.
- Enable the network ports needed for SNMP: For more information on the ports that need to be enabled for SNMP, see Turning on access for SNMP ports at the network level.

Turning on access for SNMP ports at the network level

About this task

⚠ **Caution:**

For SNMP to work, the Master Agent must be in an "Up" state and the SNMP ports must be enabled through the firewall. Use the information in this section to enable the ports needed for SNMP. To check the status of the Master Agent, select Agent Status on the server's web interface. To start the Master Agent, click **Start Agent**.

You must turn on network access for SNMP ports to allow SNMP access to Communication Manager. Use the following steps to turn on the network ports:

Procedure

1. On the server's Server Administration Interface, click **Firewall** under the Security heading.
2. On the bottom of the Firewall screen, click **Advanced Setting**.
3. Scroll down and find the following three ports used by SNMP:
    - snmp 161/tcp
    - snmp 161/udp
    - snmptrap 1
4. On all three ports listed above, select the check boxes in both the **Input to Server** and **Output to Server** columns.
5. To save the changes, click **Submit**.

SNMP traps administration

Use this section to administer the following actions for an SNMP trap destination:

- Adding an SNMP trap destination
- Displaying an administered SNMP trap
- Changing an administered SNMP trap
- Deleting an administered SNMP trap

Adding an SNMP trap destination

Procedure

1. On the server's Server Administration interface, click **SNMP Traps** under the Alarms heading.
2. Check the status of the Master Agent and do one of the following as required:
    - If the status of the Master Agent is "Up": Select **Agent Status** from the navigation bar and click **Stop Agent**. Once the Master Agent reaches a "Down" state, return to the SNMP Trap screen by clicking **SNMP Traps** on the navigation bar.
    - If the status of the Master Agent is "Down," continue to step 3
3. On the bottom of the screen, click **Add**.
4. Click the **Check to enable this destination** box.

Note:

If you do not enable this destination, you can still enter the destination information and click `Add`. The system saves the data and displays the information with the status of disabled.

5. In the **IP address** field, enter the IP address for this destination.

   Communication Manager supports SNMP v1, SNMP v2c, and SNMP v3.
6. Select the SNMP version you are using.
7. Complete the fields associated with each version of SNMP that you select:
   - **SNMP version 1**: In the **Community name** field, enter the SNMP community name.
   - **SNMP version 2c**:
     i. In the **Notification type** field: Select between trap or inform. A trap is sent without notification of delivery. An inform is sent with a delivery notification to the sending server. If a delivery notification is not received, the inform is sent again.

     ii. In the **User name** field: Enter the SNMP user name that the destination recognizes.

     iii. In the **Security Model** field, select from one of the following options:

       - **none**: Traps are sent in plan text without a digital signature.
       - **authentication**: When authentication is selected, an authentication password must be given. SNMP v3 uses the authentication password to digitally “sign” v3 traps using MD5 protocol (associate them with the user).
       - **privacy**: When privacy is selected, both an authentication password and a privacy password is used to provide user-specific authentication and encryption. Traps are not only signed as described when using authentication, but also encrypted using Data Encryption Standard (DES) protocol.

     iv. **Authentication Password** field: If you selected authentication as your security model, enter an authentication password. The password must be at least eight characters in length and can contain any characters except: ’\ &, ‘ ".

     v. **Privacy Password** field: If you selected privacy for your security model, first complete the **Authentication Password**field as described in the previous paragraph, then enter a password in the **Privacy Password** field. The password must be at least eight characters in length and can contain any characters except: ’\ &, ‘ ".

vi. **Engine ID** field: A unique engine ID is used for identification. Enter the engine ID of the designated remote server. An engine ID can be up to 24 characters in length consists of the following syntax:

- IP address: The IP address of the device that contains the remote copy of SNMP.
- Udp-port: (Optional) Specifies a User Datagram Protocol (UDP) port of the host to use.
- udp-port-number: (Optional) The socket number on the remote device that contains the remote copy of SNMP. The default number is 161.
- vrf: (Optional) Instance of a routing table.
- vrf-name: (Optional) Name of the VPN routing/forwarding (VRF) table to use for storing data.
- engineid-string: The name of a copy of SNMP.

8. Click **Add** to save the trap.
9. To add another trap, follow steps 3 through 8.
10. If you are finished adding trap destinations, you must start the Master Agent.

    To start the Master Agent, select **Agent Status** from the navigation bar and click **Start Agent**.

Displaying an administered SNMP trap

Procedure

On the server's Server Administration Interface, click **SNMP Traps**.

The administered traps display under the Current Settings heading.

Changing an administered SNMP trap

Procedure

1. On the server's Server Administration Interface, click **SNMP Traps**.
2. Check the status of the Master Agent.

   The Master Agent must be in a “Down” state before you make changes to the SNMP Traps screen.

   - If the status of the Master Agent is “Up”: Select Agent Status from the navigation bar and click **Stop Agent**. Once the Master Agent reaches a “Down” state, return to the SNMP Traps screen by clicking **SNMP Traps** on the navigation bar.

- If the status of the Master Agent is "Down," continue with 3.

3. Under the Current Settings heading on the SNMP Traps screen, click the radio button associated with the trap that you wish to change.
4. Make the changes to the trap destination and click **Change**.
5. If you are finished changing the trap destinations, you must start the Master Agent.

   To start the Master Agent, select Agent Status from the navigation bar and click **Start Agent**.

Deleting an administered SNMP trap

Procedure

1. On the server's Server Administration Interface, click **SNMP Traps**.
2. Check the status of the Master Agent.

   The Master Agent must be in a "Down" state before you make changes to the SNMP Traps screen.

   - If the status of the Master Agent is "Up": Select **Agent Status** from the navigation bar and click **Stop Agent**. Once the Master Agent reaches a "Down" state, return to the SNMP Traps screen by clicking **SNMP Traps** on the navigation bar.
   - If the status of the Master Agent is "Down," continue with 3.
3. Under the **Current Settings** heading on the SNMP Traps screen, click the radio button associated with the trap that you want to delete.
4. Click **Delete**.

   The SNMP Traps screen appears displaying the updated trap destination list.
5. If you are finished deleting the trap destinations, you must start the Master Agent.

   To start the Master Agent, select Agent Status from the navigation bar and click **Start Agent**.

SNMP agents administration

The SNMP Agents screen allows you to restrict SNMP services at the application level.

⚠ **Caution:**

The Firewall page - Advanced Settings, is used to inhibit the reception of SNMP messages at the network level. For SNMP to work, the Master Agent must be in an “Up” state and the SNMP ports must be enabled through the firewall. For more information on the Firewall page, see Turning on access for SNMP ports at the network level. For more information on how to check the status of the Master Agent, see step 2 under Administering an SNMP Agent.

The SNMP Agent screen is divided into the following sections:

- A link to view the G3-Avaya-MIB: A management information base (MIB) contains definitions and information about the properties of managed sources and services that an SNMP agent(s) supports. The G3-Avaya-MIB is used for Communication Manager. The G3-Avaya-MIB contains:

  - Object identifiers (IDs) for every Avaya object
  - A list of MIB groups and traps along with their associated varbinds
  - Configuration, fault and performance data associated with the Communication Manager server

  To view the MIB, click **G3-Avaya-MIB**.

  The G3-Avaya-MIB appears on the screen.

- IP Addresses for SNMP Access: Use this section to restrict access by all IP addresses, allow access by all IP addresses, or list IP address from which SNMP is allowed.
- SNMP User/Communities: Use this section to enable and administer the version of SNMP that you are using. Communication Manager supports SNMP v1, SNMP v2c, and SNMP v3. Each SNMP version can be enabled and disabled independently of the other versions.

Administering an SNMP Agent

About this task

⚠ **Caution:**

On the duplicated servers, you must administer an SNMP agent exactly the same on both servers.

Procedure

1. On the server’s Server Administration Interface, click **SNMP Agents**.
2. Check the status of the Master Agent.
   - If the status of the Master Agent is “up”: Select Agent Status from the navigation bar and click **Stop Agent**. Once the Master Agent reaches a “Down”

state, return to the SNMP Traps screen by clicking **SNMP Traps** on the navigation bar

- If the Master Agent is in a “Down” state, continue with step 3.

3. In the **IP Addresses for SNMP Access** section:

   Select the radio button associated with one of the following options:

   - No access: This option restricts all IP address from talking to the agent.
   - Any IP access: This option allows all IP addresses to access the agent.
   - Following IP addresses: You can specify up to five individual IP addresses that has permission to access the agent.

4. In the SNMP users/communities section: Select one or more versions of SNMP by clicking on the **Enable** box associated with the version.

   - **SNMP Version 1**:

     i. **Enable SNMP Version 1**: Check this box to enable SNMP v1. If the SNMP v1 box is enabled, SNMP v1 can communicate with the SNMP agents on the server.

     ii. **Community Name (read-only)**: When this option is selected the community or the user can query for information only (SNMPGETs).

     iii. **Community Name (read-write)**: When this option is selected the community or the user can not only query for information but can also send commands to the agents (SNMPSETs).

   - **SNMP Version 2**: Check this box to enable SNMP v2. If the SNMP v2 box is enabled, SNMP v2 can communicate with the SNMP agents on the server.

     i. **Enable SNMP Version 2**: Check this box to enable SNMP v2.

     ii. **Community Name (read-only)**: When this option is selected the community or the user can query for information only (SNMPGETs).

     iii. **Community Name (read-write)**: When this option is selected the community or the user can not only query for information but can also send commands to the agents (SNMPSETs).

   - **SNMP Version 3**: SNMP v3 provides the same data retrieval facilities as the previous versions with additional security. A User Name, authentication password, and privacy password are used to provide a secure method of authenticating the information so the device knows whether to respond to the query or not.

     i. **Enable SNMP Version 3**: Check this box to enable SNMP v3. If the SNMP v3 box is enabled, SNMP v3 can communicate with the SNMP agents on the server.

User (read-only) : Entering a user name, authentication password, and security password in this section provides the user with read functionality only.

ii. **User Name**: Enter a User Name. The User Name can be a maximum of any 50 characters with the exception of quotation marks.

iii. **Authentication Password**: Enter a password for authenticating the user. The authentication password must be a maximum of any 50 characters with the exception of quotation marks.

iv. **Privacy Password**: Enter a password for privacy. The privacy password can contain any 8 to 50 characters with the exception of quotation marks.

User (read-write): Entering a user name, authentication password, and security password in this section provides the user with read and write functionality.

v. **User Name**: Enter a User Name. The User Name can be a maximum of any 50 characters with the exception of quotation marks.

vi. **Authentication Password**: Enter a password for authenticating the user. The authentication password must be a maximum of any 50 characters with the exception of quotation marks.

vii. **Privacy Password**: Enter a password for privacy. The privacy password can contain any 8 to 50 characters with the exception of quotation marks.

5. To save the changes, click **Submit**.
6. Once you are finished adding the SNMP Agent, you must start the Master Agent.

   To start the Master Agent, select **Agent Status** from the server's Server Administration Interface and click **Start Agent**.

   Important:

   You can use the Agent Status screen to change the state of the Master Agent and to check the state of the subagents. If the subagent is connected to the Master Agent, the status of each subagent is “Up.” If the status of the Master Agent is “Down” and the status of the subagent is “Up,” the subagent is not connected to the Master Agent.

SNMP filters administration

Use the SNMP Filters screen to perform the following tasks:

- Adding an SNMP filter
- Changing an SNMP filter
- Deleting one or all SNMP filters
- Customer Alarm Reporting Options

The filters are used only for Communication Manager and determine which alarms are sent as traps to the trap receiver(s) that are administered using the SNMP Traps page. For more information on how to administer an SNMP trap, see SNMP traps administration.

Important:

Filters created by Fault and Performance Manager (FMP) do not display on the SNMP Filters screen. If you are using FMP, create the filters using the FMP application. The FMP application provide some additional capabilities that are not available using the SNMP Filters screen.

Adding an SNMP filter

About this task

Use the following steps to add a filter.

Procedure

1. On the server's Server Administration Interface, click SNMP **Filters** under the Alarms heading.
2. Click **Add**.
3. **Severity**: Select from one or more of the following alarm severities that will be sent as a trap:
    - Active
    - Major
    - Minor
    - Warning
    - Resolved
4. **Category and MO-Type**: Select the alarm category for this filter from the drop-down menu.

The **MO-Types** that display are based on the `Category` that you select. The available categories with their associated MO-Types are listed in the table on page 102.

Table 2: Category with associated MO-Type table

Category	MO-Type
adm-conn	ADM-CONN
announce	ANN-PT, ANN-BD, ANNOUNCE
atm	ATM-BCH, ATM-DCH, ATM-EI, ATM-INTF, ATM-NTWK, ATM PNC-DUP, ATM-SGRP, ATM-SYNC, ATM-TRK, ATM-WSP
bri/asai	ASAI-ADJ, ASAI-BD, ASAI-PT, ASAI-RES, ABRI-PORT, BRI-BD, BRI-PORT, BRI-SET, LGATE-AJ, LGATE-BD, LGATE-PT
cdr	CDR-LINK
data-mod	BRI-DAT, DAT-LINE, DT-LN-BD, PDMODULE, TDMODULE
detector	DTMR-PT, DETR-BD, GPTD-PT, TONE-BD
di	DI-BD, DI-PT
environ	AC-POWER, CABINET, CARR-POW, CD-POWER, EMG-XFER, EXT-DEV, POWER, RING-GEN
esm	ESM
exp-intf	AC-POWER, CARR-POWER, DC-POWER, EPN-SNTY, EXP-INTF, MAINT, SYNC, TDM-CLK, TONE-BD
ext-dev	CUST-ALM
generatr	START-3, SYNC, TDM-CLK, TONE-PT, TONE-BD
inads-link	INADS
infc	EXP-INTF
ip	MEDPRO, IPMEDPRO, MEDPORPT, H323-SGRP, H323-BCH, H323-STN, DIG-IP-STN, RDIG-STA, RANL-STA, NR-CONN, REM-FF, ASAI-IP, ADJLK-IP, SIP-SGRP
lic-file	NO-LIC, LIC-ERR
maint	MAINT
misc	CONFIG, ERR-LOG, MIS, PROC-SAN, SYSTEM, TIME-DAY
mmi	MMI-BD, MMI-LEV, MMI-PT, MMI-SYNC
mnt-test	M/T-ANL, M/T-BD, M/T-DIG, M/T-PT
modem	MODEM-BD, MODEM-PT
pkt	M/T-PKT, PKT-BUS
pms/jrnl	JNL-PRNT, PMS-LINK

Category	MO-Type
pns	DS1C-BD, DS1-FAC, EXP-INTF, FIBER-LK, PNC-DUP, SN-CONF, SNC-BD, SNC-LINK, SNC-REF, SNI-BD, SNI-PEER
pncmaint	DS1C-BD, DS1-FAC, EXP-INTF, FIBER-LK, PNC-DUP, SN-CONF,SNC-BD, SNC-LINK, SNC-REF, SNI-BD
pnc-peer	SNI-PEER
procr	PROCR
quick-st	ABRI-PT, ADXDP-PT, ANL-16-LINE, ANL-LINE, ANL-NE-LINE, ANN-PT, ANNOUNCE, ASAI-ADJ, AUDIX-PT, AUX-TRK, BRI-PT, BRI-SET, CDR-LINK, CLSFY-PT, CO-DSI, CO-TRK, CONFIG, DAT-LINE, DID-DS1, DID-TRK, DIG-LINE, DIOD-TRK, DS1-FAC, DS1C-BD, DTMR-PT, EPN-SANITY, EXP-INTF, EXP-PN, FIBER-LINK, GPTD-PT, HYB-LINE, ISDN-LNK, ISDN-TRK, JNL-PRNT, MAINT, MET-LINE, MODEM-PT, OPS-LINE, PDATA-PT, PDMODULE, PKT-BUS, PKT-INT, PMS-LINK, PMS-PRNT, PNC-DUP, PRI-CDR, S-SYN-PT, SN-CONF, SNC-BD, SNC-LNK, SNC-REF, SNI-BD, SNI-PEER, SYS-PRNT, SYSLINK, SYSTEM, TDM-BUS, TDM-CLK, TDMODULE, TIE-DS1, TIE-TRK, TONE-BD, TTR-LEV
sch-adj	SCH-ADJ
s-syn	S-SYN-BD, S-SYN-PT
stabd	ABRI-PORT, ADXDP-BD, ADXDP-PT, ANL-16-LINE, ANL-BD, ANL-LINE, ANL-NE-LINE, ASAI-ADJ, AUDIX-BD, AUDIX-PT, BRI-BD, BRI-PORT, BRI-SET, DIG-BD, DIG-LINE, HYB-BD, HYB-LINE, MET-BD, MET-LINE
stacrk	ADXDP-PT, ANL-LINE, ANL-16-LINE, ANL-NE-LINE, AUDIX-PT, DIG-LINE, HYB-LINE, MET-LINE, OPS-LINE
stations	ABRI-PORT, ADXDP-PT, ANL-16-LINE, ANL-LINE, ANL-NE-LINE, ASAI-ADJ, AUDIX-PT, BRI-PORT, BRI-SET, DIG-LINE, HYB-LINE, MET-LINE, OPS-LINE
sys-link	SYS-LINK
sys-prnt	SYS-PRNT
tdm	TDM-BUS
tone	CLSFY-BD, CLSFY-PT, DETR-BD, DTMR-PT, GPTD-PT, START-E, SYNC, TDM-CLK, TONE-BD, TONE-PT, TTR-LEV
trkbd	AUX-BD, AUX-TRK, CO-BD, CO-DS1, CO-TRK, DID-BD, DID-DS1, DID-TRK, DIOD-BD, DIOD-TRK, DS1-BD, ISDN-TRK, PE-BCHL, TIE-BD, TIE-DS1, TIE-TRK, UDS1-BD, WAE-PT
trkcrk	AUX-TRK, CO-DS1, C9-TRK, DID-DS1, DID-TRK, DIOD-TRK, ISDN-LNK, ISDN-TRK, TIE-DS1, TIE-TRK

Category	MO-Type
trunks	CO-TRK, SUX-TRK, CO-DS1, DID-DS1, DID-TRK, DIOD-TRK, ISDN-LNK, ISDN-TRK, PE-BCHL, TIE-DS1, TIE-TRK, WAE-PORT
vc	VC-BD, VC-DSPPT, VC-LEV, VC-SUMPT
vsp	MMI-BD, MMI-PT, MMI-LEV, MMI-SYNC, VC-LEV, VC-BD, VC-SUMPT, VC-DSPPT, VP-BD, VP-PT, VPP-BD, VPP-PT, DI-BD, DI-PT, MEDPRO, IPMEDPRO, MEDPROPT
wide-band	PE-BCHL, WAE-PORT
wireless	RC-BD, RFP-SYNC, WFB, CAU, WT-STA

5. MO Location: Select an MO Location from the following list:
   - Media Gateway
   - Cabinet
   - Board
   - Port
   - Extension
   - Trunk Group/Member
6. To add the filter, click **Add**.

   The Filters screen appears displaying the new filter.

Changing an SNMP filter

Procedure

1. From the server’s Server Administration Interface, click SNMP **Filters** under the Alarms heading.
2. Click the box associated with the filter you wish to change and press **Change**.
3. Make the desired changes to the filter and press **Change**.

   The **Filters** screen appears displaying the changes made to the filter.

Deleting one or all SNMP filters

Procedure

1. To delete all the filters, click **Delete All**.

The system displays a warning message asking if you are sure. If you wish to continue, click **OK**. The Filters screen appears.

2. To delete one filter, click the box associated with the filter you wish to delete and press **Delete**.

   The system displays a warning message asking if you are sure. If you wish to continue, click **OK**. The Filters screen appears with the updated list of filters.

Customer Alarm Reporting Options

The **Customer Alarm Reporting Options** sections allows you to select from one of the following reporting options:

- Report Major and Minor Communication Manager alarms only
- Report All Communication Manager alarms

Setting Customer Alarm Reporting Option

Procedure

1. Click the radio button associated with the desired reporting option.
2. Click **Update**

   The Filters screen appears displaying the selected reporting option.

Chapter 5: Processor Ethernet setup

Much like a C-LAN board, Processor Ethernet (PE) provides connectivity to IP endpoints, gateways, and adjuncts. The PE interface is a logical connection in the Communication Manager software that uses a port on the NIC in the server. There is no additional hardware needed to implement Processor Ethernet, but the feature must be enabled via license file. Type **`display system-parameters customer-options`** to verify that the **Processor Ethernet** field on the System Parameters Customer-Options (Optional Features) is set to `y`. If this field is not set to`y`, contact your Avaya representative.

During the configuration of a server, the PE is assigned to a Computer Ethernet (CE). The PE and the CE share the same IP address but are very different in nature. The CE interface is a native computer interface while the PE interface is the logical appearance of the CE interface within Communication Manager software. The interface that is assigned to the PE can be a control network or a corporate LAN. The interface that is selected determines which physical port the PE uses on the server.

Note:

The PE interface is enabled automatically on a Survivable Remote or a Survivable Core server. Do not disable the PE interface on a Survivable Remote or a Survivable Core server. Disabling the PE interface disables the Survivable Remote or Survivable Core server's ability to register with the main server. The Survivable Remote or Survivable Core server will not work if the PE interface is disabled.

In Communication Manager Release 5.2, Processor Ethernet (PE) is supported on duplicated servers for the connection of H.323 devices, H.248 gateways, SIP trunks, and most adjuncts.

The capabilities of Survivable Core servers are enhanced to support connection of IP devices to the PE interface as well as to C-LAN interfaces located in G650 (port network) gateways.

Note:

Avaya recommends that you use the following IP telephone models to ensure optimal system performance when you use Processor Ethernet on duplicated servers:

- 9610, 9620, 9630, 9640, and 9650 telephones with firmware 3.0 or later; any future 96xx models that support TTS (Time to Service) will work optimally.
- 4601+, 4602SW+, 4610SW, 4620SW, 4621SW, 4622SW, and 4625SW Broadcom telephones with firmware R 2.9 SP1 or later, provided the 46xx telephones are not in the same subnet as the servers.

All other IP telephone models will re-register in case of server interchange. The 46xx telephones will re-register if they are in the same subnet as the servers.

When PE is used on duplicated servers, it must be assigned to an IP address, Active Server IP address, that is shared between the servers. This address is known in networking terminology as an IP-alias. The active server is the only server that will respond on the IP-alias.

A Survivable Remote or a single Survivable Core server can use the Processor Ethernet interface to connect to CDR, AESVCS, and CMS. Duplicated Survivable Core servers can use the Processor Ethernet interface to connect to CDR, Messaging, and SIP Enablement Server (SES).

For more information on Survivable Core Server, see *Avaya Aura™ Communication Manager Survivable Options*, 03-603633.

Setting up the PE interface

About this task

This section contains general, high-level steps for configuring and administering the PE interface. As each system may have unique configuration requirements, contact your Avaya representative if you have questions.

Procedure

1. Load the appropriate template.
2. Configure the PE interface on the server using the server's System Management Interface:
   a. Select the interface that will be used for PE in the Network Configuration page.

      Note:

      The S8300D Server provides only one interface to configure PE.

      The Network Configuration page can be found on the server's System Management Interface select **Server (Maintenance)** > **Server Configuration**.

   b. If this is a Survivable Core or Survivable Remote Server, enter the additional information in the Configure LSP or ESS screen:
      - **Registration address at the main server** field. Enter the IP address of a C-LAN or PE interface on the main server to which the Survivable Remote or Survivable Core Server will connect. The IP address is used by the Survivable Remote or Survivable Core Server to register with the main server. In a new installation, where the Survivable Remote or the Survivable Core Server has not received the initial translation download from the main server, this address will be the only address that the Survivable Remote or the Survivable Core Server can use to register with the main server.
      - **File synchronization address of the main cluster**: Enter the IP address of a server's NIC (Network Interface Card) connected to a LAN to which the Survivable Remote or the Survivable Core Server is also connected. The Survivable Core Server or the Survivable Remote must be able to ping to the address. Consideration should be given to which interface you want

the file sync to use. Avaya recommends the use of the customer LAN for file sync.

3. On the Communication Manager System Access Terminal (SAT), enter the name for each Survivable Core Server, Survivable Remote Server, and adjunct in the IP Node Names screen.

   The SAT command is **`change node-name`**. You do not have to add the PE interface (**procr**) to the IP Node Names screen. Communication Manager adds the PE interface automatically. For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

4. For a single main server, use the IP Interfaces screen to enable H.248 gateway registration, H.323 endpoint registration, gatekeeper priority, network regions, and target socket load.

   On some platform types, the IP Interfaces screen is already configured. Use the SAT command **`display ip-interfce procr`** to see if the PE interface is already configured. If it is not, use the SAT command **`add ip-interface procr`** to add the PE interface.

5. Use the Processor Channel Assignment screen (command **`change communication-interface processor-channels`**) and the IP Services screen (**`change ip-sevices`**) to administer the adjuncts that use the PE interface on the main server:

   - Enter`p` in the **Interface Link** field on the Processor Channel Assignment screen.
   - Enter `procr` in the **Local Node** field on the IP Services screen.

6. For adjunct connectivity to a Survivable Core or Survivable Remote Server, use the Survivable Processor - Processor Channels screen to:

   - Use the same processor channels information as the main server by entering `i(nherit)` in the **Enable** field.
   - Use different translations than that of the main server by entering `o(verwrite)` in the **Enable** field. After entering `o(verwrite)` you can enter information specific to the Survivable Core or Survivable Remote Server in the remaining fields.
   - Disable the processor channel on the Survivable Core or Survivable Remote by entering `n(o)` in the **Enable** field.

7. Execute a **`save translations all`**, **`save translations ess`**, or **`save translations lsp`** command to send (file sync) the translations from the main server to the Survivable Core or Survivable Remote Server.

Network port usage

The main server(s), Survivable Remote Servers, and each Survivable Core Server, use specific TCP/UDP ports across a customer's network for registration and translation distribution. Use the information in the table on page 110 to determine which TCP/UDP ports must be open in your network for a Survivable Remote or Survivable Core Server. You must check the firewalls on your network to open the required TCP/UDP ports.

Table 3: Network port usage

Port	Used by:	Description
20	ftp data	
21	ftp	
22	ssh/sftp	
23	telnet server	
68	DHCP	
514	This port is used in Communication Manager 1.3 to download translations.	
1719 (UDP port)	The survivable server(s) to register to the main server(s).	UDP outgoing and incoming
1024 and above	Processor Ethernet	TCP outgoing
1039	Encrypted H.248	TCP incoming
1720	H.323 host cell	TCP incoming and outgoing
1956	Command server - IPSI	
2312	Telnet firmware monitor	
2945	H.248 message	TCP incoming and outgoing
5000 to 9999	Processor Ethernet	TCP incoming
5010	IPSI/Server control channel	
5011	IPSI/Server IPSI version channel	
5012	IPSI/Server serial number channel	
21873 (TCP port)	The main server(s) running Communication Manager 2.0 to download translations to the Survivable Remote Server(s).	Prior to an upgrade to Communication Manager 3.0 or later, servers running Communication Manager 2.x used port 21873 to download

Port	Used by:	Description
		translations to the Survivable Remote Server(s). Once the upgrade to 3.0 is complete and all servers are running versions of Communication Manager 3.0 or later, the main server(s) uses port 21874 to download translations and port 21873 will no longer be needed.
21874 (TCP port)	The main server(s) to download translations to the survivable servers.	A main server(s) uses port 21874 to download translations to the Survivable Core Server (s) and the Survivable Remote Server(s) on Communication Manager 3.0 and later loads.

To configure the ports on your server, click **Firewall** under the **Security** heading in the Server Administration Interface.

PE Interface configuration

Use the information in this section to configure the PE interface on the server. This section does not contain complete information on how to configure the Communication Manager server. For information on how to configure the Communication Manager server, see the installation documentation for your server type. The documentation can be found at http://support.avaya.com.

Network Configuration

Use the Network Configuration page to configure the IP-related settings for the server.

Note:

Some of the changes made on the Network Configuration page may affect the settings on other pages under **Server Configuration**. Make sure that all the pages under **Server Configuration** have the proper and related configuration information.

Use the Network Configuration page to configure or view the settings for the hostname, alias host name, DNS domain name, DNS search list, DNS IP addresses, server ID, and default gateway.

- If the configuration setting for a field is blank, you can configure that setting from the Network Configuration page.
- If the configuration setting for a field is already obtained from an external source, such as System Platform or Console Domain, that field is view-only.
- If you want to change the configuration setting obtained from an external source, you must navigate to the external source used to configure the setting.

You can also configure the IP-related settings for each Ethernet port to determine how each Ethernet port is to be used (functional assignment). Typically, an Ethernet port can be configured without a functional assignment. However, any Ethernet port intended for use with Communication Manager must be assigned the correct functional assignment. Make sure that the Ethernet port settings in the Network Configuration page match with the physical connections to the Ethernet ports. However, the labels on the physical ports may be shifted by 1. For example, eth0 maybe labeled as eth1 and eth1 maybe labeled 2 and so on. Ethernet ports may be used for multiple purposes, except for the service's laptop port. However, currently there is no service's laptop port within Communication Manager.

The number of entries for the Ethernet ports in the Network Configuration page corresponds with the number of Network interface cards (NICs) the server has. For example, if the server has three NICs, the entries for the Ethernet ports in the Network Configuration page are eth0, eth1, and eth2.

To activate the new settings in the server, you must restart Communication Manager. Make sure that you restart Communication Manager only after configuring the complete settings of the server. Too many restarts may escalate to a full Communication Manager reboot.

Important:

The IPv6 Address field is limited to a specific customer set and not for general use.

- **Host Name**: Enter or view the Communication Manager host name. The Communication Manager host name is often aligned with the DNS name of the server.
- **Alias Host Name**: Enter or view the alias host name of the server. This field is applicable only if the server is running in a duplicated mode. If the server is running in the survivable mode, make sure that you enter the alias host name.
- **DNS Domain**: Enter or view the DNS domain name of the server. For example, `company.com`
- **Search Domain List**: Enter or view the DNS search list.

  If there is more than one entry, use a comma (,) to separate each entry.
- **Primary DNS**: Enter or view the primary DNS IP address.
- **Secondary DNS**: Enter or view the secondary DNS IP address.

- **Tertiary DNS**: Enter or view the tertiary DNS IP address.
- **Server ID**: Enter or view the unique server ID (SVID) for the server.
- **Default Gateway**:
    - If the server supports IPv4 network, in the **IPv4** box, enter or view the IP version 4 default gateway address.
    - If the server supports IPv6 network, in the **IPv6** box, enter or view the IP version 6 default gateway address.

Configure the following IP-related settings for the available Ethernet port interfaces on the Network Configuration page:

- **IP Configuration**:
    - **IPv4 Address**: If the server supports IPv4 network, enter the IP version 4 address.
    - **Mask**: If you want to assign an IPv4 address, then set this field to the subnet mask required for setting up this network. The server supports the short version and long version of the mask. If you want to use the short version, then enter a numeric value from 1 to 32.
    - **IPv6 Address**: If the server supports IPv6 network, enter the IP version 6 address.
    - **Prefix**:If you want to assign an IPv6 address, then set this field to the prefix required for setting up this network. Enter a numeric value from 1 to 128.
- **Alias IP Address**:
    - **IPv4 Address**: Enter another IPv4 address that this server should respond to.
    - **IPv6 Address**: Enter another IPv6 address that this server should respond to.
- **Functional Assignment**: From the drop-down list, select one of the following options depending on how this interface should be used.
    - Corporate LAN/Processor Ethernet/Control Network
    - Corporate LAN/Control Network
    - Duplication Link
    - Services Port

Change: Click **Change** to save the configuration made on the Network Configuration page.

⚠ **Caution:**

Clicking **Change** may restart the network which can lead to a brief disconnect from the server.

Restart CM: Click **Restart CM** to activate the new settings in the server.

Important:

Click **Restart CM** only after configuring the complete settings of the server. Too many restarts may escalate to a full Communication Manager reboot.

Duplication Parameters

Use the Duplication Parameters page to configure the following settings for the server:

- Duplication type for the servers: Communication Manager supports two server duplication types—software-based duplication and encrypted software-based duplication.

  Note:

  Make sure that the server duplication type is the same for both the active and standby servers.

- Duplication parameters of the other server: Configure the< hostname>, server ID, Corporate LAN IP address<>, and the duplication link IP address for the other server.
- Processor Ethernet parameters: Configure the Processor Ethernet interchange priority level for the server and the IP address that enables the server to determine whether its Processor Ethernet interface is working or not.

To activate the new settings in the server, you must restart Communication Manager. Make sure that you restart Communication Manager only after configuring the complete settings of the server. Too many restarts may escalate to a full Communication Manager reboot.

Select Server Duplication

- **This is a duplicated server using software-based duplication**: Select this option to configure software-based duplication.

  Software-based duplication provides memory synchronization between an active and a standby server without the need for the DAL or DAJ series of duplication cards. For software duplication, the duplication messages are sent over the server duplication TCP/IP link.

- **This is a duplicated server using encrypted software-based duplication**: Select this option to configure encrypted software duplication.

  Encrypted software-based duplication provides memory synchronization between an active and a standby server by using AES 128 encryption and without any hardware assistance. If you configure encrypted software-based duplication, the BHCC call capacity of the server with encryption enabled is at least 75 percent of the BHCC call capacity of the server with encryption disabled.

Duplication Parameters for the Other Server:

- **Hostname**: Enter the host name for the other server.
- **Server ID**: Enter the unique server ID (SVID) for the other server. The range of the SVID is 1 through 256.
- **Corporate LAN/PE IP**: Provide the IP address of the Corporate LAN/Processor Ethernet for the supporting server:
    - If the server supports IPv4 network, provide the IP address in the **IPv4** text box.
    - If the server supports IPv6 network, provide the IP address in the **IPv6** text box.
- **Duplication IP**:
    - If the server supports IPv4 network, in the **IPv4** box, enter the IP address for the other server.
    - If the server supports IPv6 network, in the **IPv6** box, enter the IP address of the other server.

Processor Ethernet (PE) Parameters:

- **PE Interchange Priority**: The Processor Ethernet priority is a simple relative priority as compared to IPSIs in configurations that use both Processor Ethernet and IPSIs.

  Select the priority level from the following:
    - **HIGH**: Favors the server with the best PE SOH when PE SOH is different between servers.
    - **EQUAL**: Favors the server with the best IPSI connectivity when IPSI SOH is different between servers.
    - **LOW**: Counts the Processor Ethernet interface as one IPSI and favors the server with the best connectivity count.
    - **IGNORE**: Does not consider the Processor Ethernet in server interchange decisions.
- **IP address for PE Health Check**:
    - In the **IPv4** box, enter the IP address to enable the server to determine whether its Processor Ethernet interface is working or not.
    - In the **IPv6** box, enter the IP address to enable the server to determine whether its Processor Ethernet interface is working or not.

> **Note:**
>
> For the **IP address for PE Health Check** fields, the network gateway router is the default address. You can also use the IP address of any device on the network that responds.

Change:

Click **Change** to save the configuration of the duplicated parameters.

Restart CM:

Click **Restart CM** to activate the new settings in the server.

> ✱ **Note:**
>
> Click **Restart CM** only after configuring the complete settings of the server. Too many restarts may escalate to a full Communication Manager reboot.

Configuring a Survivable Remote or Survivable Core Server

About this task

When configuring a Survivable Core or Survivable Remote Server you must complete the Configure Server - Configure LSP or ESS screen in addition to the Network Configuration screen.

Complete the following fields in the Configure LSP or ESS screen:

Procedure

1. Select the radio button next to the correct entry to indicate if this is or not a Survivable Core server, a Survivable Remote Server.
2. In the **Registration address at the main server** field, enter the IP address of the C-LAN or PE interface of the main server that is connected to a LAN to which the Survivable Remote or Survivable Core Server is also connected.

   The IP address is used by the Survivable Remote or Survivable Core Server to register with the main server. In a new installation, where the Survivable Remote or Survivable Core Server has not received the initial translation download from the main server, this address will be the only address that the Survivable Remote or Survivable Core Server can use to register with the main server.
3. **File synchronization address of the main cluster**: Enter the IP address of a server's NIC connected to a LAN to which the Survivable Remote or Survivable Core Server is also connected.

   The Survivable Core or Survivable Remote Server must be able to ping to the address. Consideration should be given to which interface you want the file sync to use. Avaya recommends the use of the customer LAN for file sync.

Adding the PE as a controller for the H.248 gateways

About this task

Use the command **`set mgc list`** on an H.248 gateway when adding a PE-enabled S8510 or S8300D Server as the primary controller, or as an alternate controller for the gateway. The first media gateway controller on the list is the primary controller (gatekeeper).

For example, if during configuration a NIC card with IP address 132.222.81.1 is chosen for the PE interface, the **`set mgc list`** command would be:

```
set mgc list 132.222.81.1, <alt_ip-address_1>, <alt ip-address 2>
```

PE in Communication Manager Administration

Processor Ethernet administration is always performed on the main server. The Survivable Remote or Survivable Core Server receives the translations from the main server during registration or when you perform a **`save translations lsp`**, **`save translations ess`**, or **`save translations all`** command on the SAT of the main server.

When communication with the main server is lost, you can perform administration on an active Survivable Remote Server or an active Survivable Core server. In this case, the administration is temporary until the communication to the main server is restored. At that time, the Survivable Remote or Survivable Core Server registers with the main server and receives the file sync. The file sync will overwrite any existing translations.

This section outlines the screens used in the administration of Processor Ethernet. For more information on these screens, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

- IP Node Names screen

  If the PE interface is enabled in the license file, the PE interface (`procr`) automatically appears on the IP Node Names screen. You cannot add the PE interface to the IP Node Names screen.

- IP Interfaces screen

  Administer the PE interface and the C-LAN interface on the IP Interfaces screen. It is possible to have both the PE interface and one or more C-LAN boards administered on the same system. On some server types the PE interface is automatically added. To see if the PE interface is already added to your system, use the command **`display ip-interface procr`**. To add the PE interface, use the command **`add ip-interface procr`**.

Administer the PE interface on the main server if the main is an S8300D, S8510, or an S8800 and one or more of the following entities use the main server's PE interface to register with the main server:

- AE Services, CMS, CDR adjuncts
- H.248 gateways
- H.323 gateways or endpoints.

For configurations that do not use the PE interface on the main server, you do not need to administer the IP Interfaces screen. This is true even if the Survivable Core or Survivable Remote Server is using the PE interface. The IP Interfaces screen is automatically populated for a Survivable Core or Survivable Remote Server.

- Survivable Processor screen

The Survivable Processor screen is used to add a new Survivable Remote Server and also provides a means to connect one of the three supported adjuncts (CMS, CDR, AESVCS) to a Survivable Remote or Survivable Core Server. The Survivable Processor screen is administered on the main server. The translations are sent to the Survivable Core or Survivable Remote Server during a file sync. After the file sync, the information on the Survivable Processor screen is used by the Survivable Remote or Survivable Core Server to connect to a CMS, an AESVCS, or a CDR.

Survivable Core Servers administration for PE

If there is a Survivable Core Server in the configuration, you must add the Survivable Core Server using the Survivable Processor screen. For more information on administering the Survivable Core Server on the Survivable Processor screen, see *Avaya Aura™ Communication Manager Survivable Options*, 03-603633.

Survivable Remote Servers administration for PE

Survivable Remote Servers are administered using the Survivable Processor screen. For more information on administering a Survivable Remote Server, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Adjuncts with PE

For the single main server, adjuncts that use the C-LAN can use the PE interface of the main server for connectivity to the main server. For the Survivable Remote and Survivable Core Servers, there are three adjuncts, the CMS, AESVCS, and the CDR, that are supported using the Survivable Remote or Survivable Core Server's PE interface. This section provides a high-level overview of the adjuncts supported by the Survivable Core and Survivable Remote Servers and how they are administered to use the PE interface.

- **Survivable CMS**

  Starting with CMS Release 13.1, you can use a Survivable CMS co-located at the site of the Survivable Core or Survivable Remote Server. A Survivable CMS is a standby CMS that collects data from a Survivable Remote or Survivable Core Server when the main server is not operational or when the customer is experiencing a network disruption. A Survivable CMS should not be located at the same location as the main server.

  During normal operations, the Survivable CMS has a connection to the Survivable Core or Survivable Remote Server, but does not collect data or support report users. Only the main CMS server collects data. When a Survivable Core Server assumes control of one or more port networks, or a Survivable Remote Server is active, the Survivable Core Server and/or the Survivable Remote Server sends data to the Survivable CMS.

- **CDR**

  The server initiates the connection to the CDR unit and sends call detail information over the configured link. The link remains active at all times while the CDR unit waits for data to be sent by a connected server. In the case of a Survivable Core or Survivable Remote Server, data will not be sent until the survivable server becomes active. Some CDR units can collect data from multiple servers in a configuration, separately or all at once. For information on the capability of your CDR unit, check with your CDR vendor.

  The CDR unit is administered on the IP Services screen. To use the PE interface, `procr` must be entered in the **Local Node** field.

- **AESVCS**

  AESVCS (Application Enablement Services) supports connectivity to a maximum of 16 servers. Since AESVCS cannot tell which server is active in a configuration, it must maintain a constant connection to any server from which it might receive data. An Avaya S8xxx Server “listens” for AESVCS after it boots up. The AESVCS application establishes the connection to the server.

  If the adjunct terminates solely on the main server’s PE interface, you do not have to administer the Survivable Processor screen. If AESVCS connects to a Survivable Remote or Survivable Core Server, you must administer the Survivable Processor screen in addition to the IP Services screen.

Load balancing for PE

You can load balance the H.323 endpoint traffic across multiple IP interfaces. The IP Interfaces screen contains the fields needed to load balance the IP interface.

Note:

The 4606, 4612, and 4624 telephones do not support the load balancing feature of the TN2602AP circuit pack.

Use the following guidelines to load balance the H.323 endpoints:

1. Load balancing starts with placing the C-LANs and the PE interface into a network region using the **Network Region** field.
2. Within the network region, further load balancing is done by entering a priority in the **Gatekeeper Priority** field. This field appears only if the **Allow H.323 Endpoint** field is set to `y`. You can have more than one IP interface administered at the same value in the **Gatekeeper Priority** field within a region. For example, you could have two C-LANs administered as a in the **Gatekeeper Priority** field.

   Valid values for the **Gatekeeper Priority** field range from `1` to `9`, with `1` being the highest. Within a network region, the system uses the highest Gatekeeper Priority IP interface first.
3. The number that is entered in the **Target socket load** or the **Target socket load and Warning level** field is the maximum number of connections you want on the interface. A socket represents a connection of an endpoint to the server. As endpoints connect, the load balancing algorithms direct new registrations to interfaces that are less loaded. The current load is unique to each interface and is the ratio of currently used sockets to the number administered in this field. Communication Manager tries to keep the ratio used by each interface the same. Note that this is a “target” level, and that Communication Manager might use more sockets than specified in the field.

   If there is only one ip-interface within a priority, the **Target socket load** or the **Target socket load and Warning level** field is no longer used for load balancing. A number can be entered in this field to receive an error or a warning alarm if the targeted value is exceeded.

Alternate Gatekeeper List (AGL) priorities

The alternate gatekeeper list is used for H.323 endpoints when they cannot reach their primary gatekeeper. The **Gatekeeper Priority** field and the **Network Region** field on the IP Interfaces screen determines the priority of the PE interface or the C-LAN on the alternate gatekeeper list. For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878. For more information about the **Gatekeeper Priority** field, see Load balancing for PE.

Chapter 6: Managing Telephones

Installing New Telephones

Simple administration allows you to plug a telephone into a jack and dial a sequence to start up service to the telephone. The dialing sequence sets up an association between the telephone and the corresponding station administration.

Security alert:

If you do not manage this feature carefully, its unauthorized use might cause you security problems. Consult the *Avaya Products Security Handbook* for suggestions on how to secure your system and find out about obtaining additional security information. For traditional instructions, see *Installing New Telephones*.

Before You Start

Procedure

1. On the Feature-Related System Parameters screen, be sure the **Customer Telephone Activation (CTA) Enabled** field is y and the **TTI Enabled** field is y
2. Complete the Station screen for the new telephone and type `x` in the **Port** field.

   Note:

   The telephone type must match the board type. For example, match a two-wire digital telephone with a port on a two-wire digital circuit pack. Use this procedure with all circuit-switched telephones except BRI (ISDN) and model 7103A.

   Caution:

   You can destroy your hardware if you attempt to connect an analog telephone to a digital port.

   To associate a telephone with existing x-port station administration, complete the following steps from the telephone you want to install:

3. Plug the telephone into the wall jack.
4. Lift the receiver and continue if you hear the dial tone.
5. Dial `#*nnnn`, where nnnn is the extension number of the telephone you are installing.

6. Hang up after you receive the confirmation tone.
7. Dial a test call to confirm that the telephone is in service.

   If possible, call a telephone with a display so the person answering can confirm that you entered the correct extension number.
8. Repeat the process until all new telephones have been installed.
9. For security reasons, you should disable this feature when you are done. At the system administration terminal type change system-parameters features to access the Feature-Related System Parameters screen.
10. Type `n` in the **Customer Telephone Activation (CTA) Enabled** field.
11. Press `Enter` to save your changes.
12. Type **`save translations`**.
13. Press `Enter` to permanently save the changes.

    Fixing problems: If you misdial and the wrong extension is activated for the telephone you are using, use the terminal translation initialization (TTI) unmerge feature access code to “uninstall” the telephone before you try again.

Adding new telephones

When you are asked to add a new telephone to the system, what do you do first? To connect a new telephone you need to do three things:

About this task

Before you can determine which port to use for the new telephone, you need to determine what type of telephone you are installing, what ports are available, and where you want to install the telephone.

Procedure

1. Find an available port .
2. Wire the port to the cross-connect field or termination closet.
3. Tell the telephone system what you are doing.

Related topics:

Managing Telephones on page 121

Gathering necessary information

Procedure

1. Determine whether the telephone is an analog, digital, ISDN, or hybrid set. You can also administer a virtual telephone, one without hardware at the time of administration.

   You need this information to determine the type of port you need, because the port type and telephone type must match.

2. If you do not know what type of telephone you have, see the **Type** field on the Station screen for a list of telephones by model number.

3. Record the room location, jack number, and wire number.

   You might find this information on the jack where you want to install the telephone, recorded in your system records, or from the technician responsible for the physical installation.

4. To view a list of boards on your system, type `list configuration station`.
   The available boards (cards) and ports appear.

5. Press `Enter`.
   The System Configuration screen appears. The System Configuration screen shows all the boards on your system that are available for connecting telephones. You can see the board number, board type, circuit-pack type, and status of each board's ports.

6. Choose an available port and record its port address.
   Each port that is available or unassigned is indicated by a “u”. Choose an available port from a board type that matches your telephone type (such as a port on an analog board for an analog telephone). Every telephone must have a valid port assignment, also called a port address. The combined board number and port number is the port address. So, if you want to attach a telephone to the 3rd port on the 01C05 board, the port address is 01C0503 (01=cabinet, C=carrier, 05=slot, 03=port).

   Note:

   If you add several telephones at one time, you might want to print a paper copy of the System Configuration screen.

7. To print the screen to a printer attached to the system terminal, type `list configuration station print`

8. Press `Enter`.

9. To print to the system printer that you use for scheduled reports, type `list configuration station schedule immediate.`

10. Press `Enter`.
11. Choose an extension number for the new telephone.

    The extension you choose must not be assigned and must conform to your dial plan. You should also determine whether this user needs an extension that can be directly dialed (DID) or reached via a central telephone number. Be sure to note your port and extension selections on your system's paper records.

Connecting the Telephone physically

Once you have collected all the information, you are ready to physically wire the port to the cross-connect field.

If you have an Avaya technical support representative or on-site technician who completes the physical connections, you need to notify them that you are ready to add the telephone to the system. To request that Avaya install the new connections, call your Avaya technical support representative to place an order.

If you are responsible for making the connections yourself and if you have any questions about connecting the port to the cross-connect field, see your system installation guide. Now you are ready to configure the system so that it recognizes the new telephone.

Obtaining display labels for telephones

Instructions for downloading telephone display labels

About this task

You will need display labels for each telephone type that you will install.

Procedure

1. Set the **Display Language** field on the Station screen to English, Spanish, Italian, French, user-defined, or unicode.

   Note:

   Unicode display is only available for Unicode-supported telephones. Currently, the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones support Unicode display. Unicode is also an option for the 2420J telephone when **Display Character Set** on the System Parameters Country-Options screen is Katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide, 555-250-701.*

2. For a Eurofont character display for the 2420/2410 telephone, set the **Display Character Set** field on the System-Parameters Country-Options screen to Eurofont.

3. For a Katakana character display for the 2420/2410 telephone, set the **Display Character Set** field on the System-Parameters Country-Options screen to Katakana.

Adding a new station

Before you begin

Make sure the extension number that you are about to use conforms to your dial plan.

About this task

The information that you enter on the Station screen advises the system that the telephone exists and indicates which features you want to enable on the telephone. Communication Manager allows customers enter extensions with punctuation on the command line. Punctuation is limited to dashes (hyphens) and dots (periods). Communication Manager cannot process a command like `add station 431 4875`. You must format a command in one of these ways:

- add station 431-4875
- add station 431.4875
- add station 4314875

Procedure

1. To access the Station screen for the new telephone choose one the following actions.

    - Type `add station nnnn`, where nnnn is the extension for the new telephone.
    - Type `add station next` to automatically use the next available extension number.

      Note:

      If you have **Terminal Translation Initialization (TTI)** enabled, you might receive the following error message when attempting to add a new station:
      ```
      No station/TTI port records available; 'display capacity' for their usage
      ```
      .

    If your receive this error message, choose one or more of the following actions.

    - Remove any DCP or Analog circuit packs that have no ports administered on them.

   - If you are not using TTI or any related feature (such as PSA or ACTR), set the **Terminal Translation Initialization (TTI) Enabled?** field on the Feature Related System Parameters screen ton.
   - Contact your Avaya technical support representative. For more information on TTI, see Terminal Translation Initialization in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.
   - For more information on the System Capacity screen, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

2. Press `Enter`.
   When the Station screen appears, you see the extension number and some default field values.
3. Type the model number of the telephone into the **Type** field. For example, to install a 6508D+ telephone, type `6480D+` in the **Type** field.

   Note:

   The displayed fields might change depending on the model you add.
4. Type the port address in the **Port** field.

   Note:

   Port 1720 is turned off by default to minimize denial of service situations. This applies to all IP softphones release 5.2 or later. You can change this setting, if you have root privileges on the system, by typing the command: `/opt/ecs/sbin ACL 1720 on` or `off`.
5. Type a name to associate with this telephone in the **Name** field.
   The name you enter displays on called telephones that have display capabilities. Some messaging applications, such as INTUITY, recommend that you enter the user’s name (last name first) and their extension to identify the telephone. The name entered is also used for the integrated directory.

   Tip:

   To hide a name in the integrated directory, enter two tildes (~~} before the name when you assign it to the telephone, and set **Display Character Set** on the System Parameters Country-Options screen to Roman. This hides the name in the integrated directory. The tildes are not displayed with Caller ID name. Note that this is the only method to hide a name in the integrated directory. Also, if a name is entered with only one tilde (~), the name is converted to Eurofont characters.

   Note:

   For 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones, the **Name** field is supported by Unicode language display. You must be using ASA or MSA. For more information on Unicode language display, see *Administering Unicode display.*. Unicode is also an option for the 2420J telephone when **Display Character Set** on the System Parameters Country-Options screen is Katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide, 555-250-701.*

6. Press `Enter` to save your changes.

Changing a station

About this task

You can make changes to a new telephone, such as assigning coverage path or feature buttons.

Procedure

1. Enter `change station nnnn` where nnnn is the extension of the new telephone.
2. Change the necessary fields, then press `Enter`.

Duplicating Telephones

About this task

A quick way to add telephones is to copy the information from an existing telephone and modify it for each new telephone. For example, you can configure one telephone as a template for an entire work group. Then, you merely duplicate the template Station screen to add all the other extensions in the group.

Note:

Only telephones of the same model can be duplicated. The `duplicate` command copies all the feature settings from the template telephone to the new telephones.

Procedure

1. Type `display station nnnn`, where nnnn is the extension of the Station screen you want to duplicate to use as a template.
2. Press `Enter`.
3. Verify that this extension is the one you want to duplicate.

4. Press `Cancel` to return to the command prompt.
5. Type `duplicate station nnnn`, where nnnn is the extension you want to duplicate; then press `Enter`.
   The system displays a blank duplicate Station screen.

   Alternately, you can duplicate a range of stations by typing `duplicate station <extension> start nnnn count <1-16>`, where <extension> represents the station you want to duplicate, nnnn represents the first extension number in a series, and count <1-16> represents the number of consecutive extensions after the start extension to create as duplicates.

   > **Note:**
   >
   > If you want to duplicate the settings of another station, but need to change the port or station type, you must individually administer each station after creating the duplicates.
6. Type the extension, port address and telephone name for each new telephone you want to add.

   The rest of the fields on the Station screen are optional. You can complete them at any time.
7. Press `Enter`.
   Changes are saved to system memory.
8. To make changes to these telephones, such as assigning coverage paths or feature buttons, type `change station nnnn`, where nnnn is the extension of the telephone that you want to modify; then press `Enter`.

Adding multiple call center agents

About this task

You can add multiple call center agents, all with the same settings, based on an agent that is already administered.

Procedure

1. Enter `command duplicate agent-loginID` and the extension of the agent you want to duplicate.
2. Select `Start` and enter the extension you want to use for the first new agent
3. Select `count` and the number of agents you want to add.
4. Fill in the information on the Agent LoginID screen.

For more information, see *Avaya Call Center Release 4.0 Automatic Call Distribution (ACD) Guide, 07-600779*.

Using an alias

About this task

Not every telephone model or device has a unique Station screen in the system. You might have to use an available model as an “alias” for another. If you need to enter a telephone type that the system does not recognize or support, use an alias. Defining aliases is also a useful method to identify items that act as analog stations on Communication Manager, such as fax machines, modems, or other analog device.

If you purchase a telephone model that is newer than your system, you can alias this telephone to an available model type that best matches the features of your new telephone. See your telephone’s manual to determine which alias to use. If your manual does not have this information, you can contact the DEFINITY helpline for an appropriate alias.

For example, we will create two aliases: one to add a new 6220 telephone and one to add modems to our system.

Procedure

1. See your new telephone’s manual to find the correct alias.

   In our example, we find that the 6220 should be administered on an older system as a 2500 telephone.

2. Type `change alias station`.

3. Press `Enter`.
   The Alias Station screen appears.

4. Type `6220` in the **Alias Set Type** field.

   This is the name or model of the unsupported telephone.

5. Type `2500` in the **Supported Set Type** field.

   This is the name or model of the supported telephone.

6. Type `modem` in the **Alias Set Type** field.

   You can call the alias set anything you like. Once you define the alias, you can use the alias set in the **Type** field on the Station screen.

7. Type `2500` in the **Supported Set Type** field.

   Entering 2500 indicates to the system that these models are basic analog devices.

8. Press `Enter` to save your changes.

Now you can follow the instructions for adding a new telephone (or adding a fax or modem). Avaya Communication Manager now recognizes the new type (6220 or modem) that you enter in the **Type** field.

Be sure to see your telephone's manual for instructions on how to set feature buttons and call appearance buttons.

Note:

If you need to use an alias for a telephone, you might not be able to take advantage of all the features of the new telephone.

Customizing your Telephone

This section provides recommendations for setting up or enhancing your personal telephone. You need a telephone that is powerful enough to allow you to use all the features you might give to other employees. You might want to add feature buttons that allow you to monitor or test the system, so that you can troubleshoot the system from your telephone.

It will be much easier to monitor and test your system if you have a telephone with:

- A large multi-button display (such as 8434D or 8410D)
- A class of service (cos) that has console permissions
- The following feature buttons
  - ACA and Security Violations (assign to lamp buttons)
  - Busy verify
  - Cover message retrieval button
  - Major/minor alarm buttons
  - Trunk ID buttons
  - Verify button

Once you select a telephone, you'll want to determine if you want to place this telephone at your desk or in the server room. If the telephone is in the server room (near the system administration terminal), you can quickly add or remove feature buttons to test features and facilities. You might decide that you want a telephone at both your desk and in the server room — it's up to you.

You might also find it handy to set up multiple telephones for testing applications and features before you provide them to users. You might want to have a telephone that mimics each type of user telephone in your organization. For example, if you have four basic telephone templates, one for executives, one for marketing, one for technicians, and one for other employees, you might want to have examples of each of these telephones so you can test new features or options. Once you are satisfied that a change works on the test telephone, you can make the change for all the users in that group.

Upgrading telephones

About this task

If you want to change telephone types for a user and do not need to change locations, you can just access the Station screen for that extension and enter the new model number.

Note:

This method can be used only if the new telephone type matches the existing port type (such as digital telephone with a digital port).

For example, if a user at extension 4556 currently has a 7410+ telephone and you want to replace it with a new 8411D telephone:

Procedure

1. Type `change station 4556`.
2. press `Enter`.
   The Station screen for 4556 appears.
3. Overwrite 7410+ with `8411D` in the **Type** field.
4. Press `Enter`.
   Now you can access the functions and feature buttons that correspond to an 8411D telephone.

Swapping telephones

About this task

You will often find that you need to move or swap telephones. For example, employees moving from one office to another might want to bring their telephones. In this case, you can use X ports to easily swap the telephones.

In general, to swap one telephone (telephone A) with another telephone (B), you change telephone A’s port assignment to x, change telephone B’s port assignment to A’s old port, and, finally, change the x for telephone A to B’s old port. Note that these swapping instructions work only if the two telephones are the same type (both digital or both analog, etc.).

For example, to swap telephones for extension 4567 (port 01C0505) and extension 4575 (port 01C0516), complete the following steps:

Procedure

1. Type `change station 4567`.
2. Press `Enter` .
3. Record the current port address (01C0505) and type **x** in the **Port** field.
4. Press `Enter` to save your changes.
5. Type `change station 4575`.
6. Press `Enter` .
7. Record the current port address (01C0516)
8. Type `01C0505` in the **Port** field.
9. Update the **Room** and **Jack** fields.
10. Press `Enter` to save your changes
11. Type `change station 4567` again.
12. Press `Enter`.
13. Type `01C0516` in the **Port** field

    This is the port that used to be assigned to extension 4575
14. Update the **Room** and **Jack** fields.
15. Press `Enter` to save your changes.
16. Physically unplug the telephones and move them to their new locations.

    When you swap telephones, the system keeps the old button assignments. If you are swapping to a telephone with softkeys, the telephone could have duplicate button assignments, because softkeys have default assignments. You might want to check your button assignments and modify them as necessary.

Automatic Customer Telephone Rearrangement

Automatic Customer Telephone Rearrangement (ACTR) allows a telephone to be unplugged from one location and moved to a new location without additional administration in Avaya Communication Manager. Communication Manager automatically associates the extension to the new port. ACTR works with 6400 Serialized telephones and with the 2420/2410 telephones. The 6400 Serialized telephone is stamped with the word “Serialized” on the faceplate for easy identification. The 6400 Serialized telephone memory electronically stores its own part ID (comcode) and serial number, as does the 2420/2410 telephone. ACTR uses the stored information and associates the telephone with new port when the telephone is moved.

ACTR is an enhancement to Terminal Translation Initialization (TTI), Personal Station Access (PSA), Customer Telephone Activation (CTA). ACTR makes it easy to identify and move telephones.

⚠ **Caution:**

When a telephone is unplugged and moved to another physical location, the **Emergency Location Extension** field must be changed for that extension or the USA Automatic Location Identification database must be manually updated. If the **Emergency Location Extension** field is not changed or if the USA Automatic Location Identification database is not updated, the DID number sent to the Public Safety Access Point (PSAP) could send emergency response personnel to the wrong location.

On the Feature-Related System Parameters screen, set the **Terminal Translation Initialization (TTI) Enabled** field toy and the **TTI State** field to voice.

Note:

When a telephone is moved, if there is any local auxiliary power (a power supply plugged into a local AC outlet), the telephone must be plugged into an AC outlet at the telephone's new location. A telephone with remote auxiliary power must be supplied remote auxiliary power at its new location. If you do not supply auxiliary power in either case after a telephone is moved, some optional adjuncts (for example, an expansion module) do not operate.

When you enter always or once in the **Automatic Moves** field on the Station screen, Communication Manager adds the extension to its ACTR Move List database. When the telephone is plugged in, Communication Manager asks the telephone for its serial number and records the serial number on the ACTR Move List. If you change the entry in the **Automatic Moves** field from always or once to no, Communication Manager removes the extension from the Move List.

How calls are processed during a move

When a telephone is unplugged while on a call, and a 6400 Serialized telephone or a 2420/2410 telephone that is administered for automatic moves is plugged into the port within 60 seconds.

- Both extensions are placed in idle state
- Active calls on either extension are dropped, unless the call is active on a bridged appearance at some other telephone
- Held calls remain in a hold state
- Any calls ringing on either extension instantly proceed to the next point in coverage or station hunting path, unless the call is ringing on a bridged appearance at some other telephone
- User actions that were pending when the new telephone was plugged in are aborted

You can use the `list station movable` command to keep track of extensions on the move list. Once you reach the maximum number, Communication Manager does not allow additional extensions.

Using ACTR to move telephones

Before you begin

- Be sure the **TTI** field on the Feature-Related System Parameters screen is set to y.
- Before you move a telephone in your system, set the **TTI State** field to voice on the Feature-Related System Parameters screen.

About this task

You can allow a telephone to be unplugged from one location and moved to a new location without additional administration on Avaya Communication Manager. For example, to allow moves anytime for a telephone at extension 1234:

Procedure

1. Type `change station 1234`.
2. Press `Enter`.
3. Move to the **Automatic Moves** field
4. Type `always` in the **Automatic Moves** field.
5. Press `Enter` to save your changes.

Terminal Translation Initialization

Terminal Translation Initialization (TTI) allows you to merge an x-ported station to a valid port by dialing a TTI merge code, a system-wide security code, and the x-port extension from a telephone connected to that port. TTI also allows you to separate an extension from its port by dialing a similar separate digit sequence. This action causes the station to revert to an x-port.

TTI can be used for implementing telephone and data module moves from office to office. That is, you can separate a telephone from its port with TTI, unplug the telephone from the jack, plug in the telephone in a jack in a different office, and merge the telephone to its new port with TTI.

If you are moving telephones and concerned about security, you might also want to see *Setting up Personal Station Access* for more information about setting the security code for each extension.

Security alert:

If you do not manage this feature carefully, its unauthorized use might cause you security problems. For example, someone who knows the TTI security code could disrupt normal business functions by separating telephones or data terminals. You can help protect against this action by frequently changing the TTI security code. You can further enhance system security by removing the feature access code (FAC) from the system when it does not need to be used (for example, there are no moves going on at present). Consult the *Avaya Products Security Handbook* for additional steps to secure your system and find out about obtaining information regularly about security developments.

Merging an extension with a TTI telephone

Before you begin

Before you can merge a telephone, you must set the **TTI State** field to voice on the Feature-Related System-Parameters screen. You also must set the extension to match the port type of the TTI port making the merge request. For example, a digital telephone type can merge only to a port on a digital board.

About this task

⚠ **Caution:**

When a telephone is unplugged and moved to another physical location, the **Emergency Location Extension** field must be changed for that extension or the USA Automatic Location Identification database must be manually updated. If the **Emergency Location Extension** field is not changed or if the USA Automatic Location Identification database is not updated, the DID number sent to the Public Safety Network could send emergency response personnel to the wrong location.

✱ **Note:**

You cannot use TTI to change a virtual extension.

⚠ **Caution:**

You can destroy your hardware if you attempt to connect an analog telephone to a digital port.

Procedure

1. Dial the TTI merge FAC
   - If the code is correct, you receive the dial tone.
   - If the code is not correct, you receive the intercept tone.
2. Dial the TTI security code from the telephone you want to merge.
   - If the code is correct, you receive the dial tone.
   - If the code is not correct, you receive the intercept tone.
3. Dial the extension of the telephone you want to merge.

- If the extension is valid, you receive confirmation tone, which might be followed by dial tone. (It is possible to receive the intercept tone immediately following the confirmation tone. If this happens, you need to attempt the merge again.)
- If the extension is valid, but the extension is being administered, you receive the reorder tone. Try the merge again later.
- If the extension is invalid, you receive the intercept tone.
- If the system is busy and cannot complete the merge, you receive the reorder tone. Try the merge again later.
- If the telephone has a download status of pending, you receive the reorder tone. You need to change the download status to complete to successfully complete the TTI merge.

Separating TTI from a telephone

Procedure

1. Dial the TTI separate FAC.
2. Dial the TTI security code.
    - If the code is correct, you receive the dial tone.
    - If the code is not correct, you receive the intercept tone.
3. Dial the extension of the telephone to be separated.
    - If you have dialed the extension of the telephone currently merged with this telephone, you receive the confirmation tone.
    - If you have dialed the extension of the telephone currently merged with this telephone, but the extension is being administered, you receive reorder tone. Try the separation again later.
    - If you have not dialed the extension of the telephone currently merged with this telephone, you receive the intercept tone.
    - If the system is busy and cannot complete the separation, you receive the reorder tone. Try the separation again later.

Troubleshooting TTI

If you are having difficulty using TTI, you might want to review the following system restrictions

Problem	Restriction
The **TTI Ports** field on the System Capacity screen (type display capacity) shows the number of TTI ports used in a server running Communication Manager.	This field shows only the number of TTI ports being administered. If a TTI exceeds the maximum number of ports, the port is not administered and cannot be added. In that case, a telephone cannot be added. For details on the System Capacity screen, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431. BRI endpoints are only counted as one TTI port. For example, for every two BRI endpoints, one TTI port is counted. As such, you can have two telephones assigned to one port. If either endpoint is administered, the TTI port count is reduced by 1.
The total number of translated telephones and Voice TTI ports in a system is limited to the maximum number of administered telephones supported in the system.	The total number of translated data terminals and Data TTI ports in a system is limited to the maximum number of administered data modules allowed in the system.
Set the **TTI State** field to voice and then set the **TTI State** field to data. When you use this order, voice and then data, you reduce the chance of a user trying to use TTI on a data-only terminal that does not have TTI port translation	This can happen when the number of telephones allowed by the system is twice the number of data terminals. For example, if the system limit for telephones is 15,000 and 7,500 for data, then when TTI was turned on for data first, only the first 7,500 unadministered ports would get TTI port translations.
When TTI is activated for the system, these actions take place	• If the **TTI State** field was previously activated but in a different state (such as, a voice to data state), the old TTI translations are removed and the new ones added on a board by board basis • If the **TTI State** field is set to voice, then default TTI translations are generated for every unadministered port on all digital, hybrid, and analog boards.

Problem	Restriction
	• If the **TTI State** field is set to data, then default TTI translations are generated for every unadministered port on all digital and data line boards in the system. • Whenever a new digital board is inserted when the system is in TTI Data mode, or when a digital, hybrid, or analog board is inserted when the system is in TTI Voice mode, the unadministered ports on the board become TTI ports. • When TTI is deactivated, all translation for the TTI ports are removed in the system; the ports return to an unadministered state.

Removing telephones

Before you begin

Before you physically remove a telephone from your system, check the telephone's status, remove it from any group or usage lists, and then delete it from the system's memory. For example, to remove a telephone at extension 1234:

Procedure

1. Type `status station 1234`.
2. Press `Enter`.
   The General Status screen appears.
3. Make sure that the telephone:
   a. is plugged into the jack
   b. is idle (not making or receiving calls)
   c. has no messages waiting
   d. has no active buttons (such as **Send All Calls** or **Call Forwarding**)
4. Type `list groups-of-extension 1234`.
5. Press `Enter`.
   The Extension Group Membership screen shows whether the extension is a member of any groups on the system.
6. Press Cancel.
7. If the extension belongs to a group, access the group screen and delete the extension from that group.
   If extension 1234 belongs to pickup group 2, type `change pickup group 2` and delete the extension from the list.
8. Type `list usage extension 1234`.

9. Press `Enter`.
   The Usage screen shows where the extension is used in the system.
10. Press `Cancel`.
11. If the extension appears on the Usage screen, access the appropriate feature screen and delete the extension.
    If extension 1234 is bridged onto extension 1235, type `change station 1235` and remove the appearances of 1234.
12. Type `change station 1234`.
13. Press `Enter`.
14. Type `remove station 1234`.
15. Press `Enter`.
    The system displays the Station screen for this telephone so you can verify that you are removing the correct telephone.

    Tip:

    Be sure to record the port assignment for this jack in case you want to use it again later
16. If this is the correct telephone, press `Enter`.
    a. If the system responds with an error message, the telephone is busy or still belongs to a group.
    b. Press `Cancel` to stop the request, correct the problem.
    c. Enter `remove station 1234` again
17. Remove the extension from voice mail service if the extension has a voice mailbox.
18. Type `save translations`.
19. Press `Enter` to save your changes

    Note:

    You do not need to delete the extension from coverage paths. The system automatically adjusts coverage paths to eliminate the extension.

Next steps

Now you can unplug the set from the jack and store it for future use. You do not need to disconnect the wiring at the cross-connect field. The extension and port address remain available for assignment at a later date.

Once you successfully remove a set, that set is permanently erased from system memory. If you want to reactivate the set, you have to add it again as though it were a new telephone.

Adding a fax or a modem

About this task

Connecting a fax machine or modem to your system is similar to adding a telephone, with a few important exceptions. If you have not added a telephone, you might want to read *Adding Telephones*.

Because the system does recognize the concept of “fax” or “modem”, you need to administer these items as basic analog stations. You can merely use the supported station type 2500 (analog, single line).

Alternatively, you can create aliases to the 2500 for fax machines and modems. If you want to be able to create reports that indicate which stations are faxes or modem, you should create aliases for these items. For more information about aliasing, see *Using Alias*.

For this example, let us assume that we have already defined an alias for “fax” as a 2500 and that we now want to add a fax machine to extension 4444.

Procedure

1. Type `add station 4444`.
2. Press `Enter`.
3. In the **Type** field, type `fax`.
4. In the **Port** field, type the port address.
5. In the **Name** field, type a name to associate with this fax.
6. Move to the **Data Restriction** field and type `y`.

   Entering y in this field prevents calls to and from this extension from being interrupted by tone signals. This is important for fax machines and modems as these signals can disrupt transmissions of data.
7. In the **Distinctive Audible Alert** field, type n.

   This eliminates the distinct 2-burst ring for external calls, which often interferes with the auto-answer function on fax machines or modems.
8. Press `Enter` to save changes.

Enabling transmission over IP networks for modem, TTY, and fax calls

Before you begin

The ability to transmit fax, modem, and TTY calls over IP trunks or LANs and WANs assumes that the endpoints sending and receiving the calls are connected to a private network that uses H.323 trunking or LAN connections between gateways and/or port networks. This type of transmission also assumes that calls can either be passed over the public network using ISDN-PRI trunks or passed over an H.323 private network to Communication Manager switches that are similarly enabled. As a result, it is assumed that you have assigned, or will assign, to the network gateways the IP codec you define in this procedure. For our example, the network region 1 will be assigned codec set 1, which you are enabling to handle fax, modem, and TTY calls.

Procedure

1. Type `ip-codec-set 1`.
2. Press `Enter`.
   The IP Codec Set screen appears.
3. Complete the fields as required for each media type you want to enable.
4. Press `Enter`.

   For more information on modem/fax/TTY over IP, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

IP Softphones

Avaya IP Softphones enable the end user to control telephone calls directly from a personal computer (PC). An end user can log in remotely to your company's server running Avaya Communication Manager and then make and receive telephone calls from the telephone extension.

Avaya IP Softphones supports the following modes:

- **Road-Warrior**

  You typically use this mode for laptop users who are travelling. In this mode, the PC LAN connection carries both the call control signaling and the voice path. Because the audio portion of the voice call is handled by the PC, you must have some kind of audio device (e.g., handset, headset) PC to provide the audio connection.

- **Telecommuter or Avaya IP Agent**

  For the telecommuter or Avaya IP Agent mode, you make two separate connections to the Avaya DEFINITY server. The signaling path is carried over an IP network and the voice path is carried over the standard circuit-switched telephone network (PSTN). Since you are using a telephone for audio, you do not need an H.323 PC audio application.

  The telecommuter mode uses the Avaya IP Softphone interface (on the user's PC) and a standard telephone. The Avaya IP Agent mode uses the Avaya IP Agent interface (on the agent's PC) and a call center telephone.

- **Native H.323 (only available with Avaya IP Softphone R2)**

  The stand-alone H.323 mode enables travelers to use some Communication Manager features from a remote location. This mode uses a PC running an H.323 v2-compliant audio application, such as Microsoft NetMeeting. The H.323 mode controls the call signaling and the voice path. However, since it does not use the IP Softphone interface, this configuration is capable of operating only as an analog or single-line telephone making one call at a time without any additional assigned features. You can provide stand-alone H.323 users only features that they can activate with dial access codes.

- **Control of IP Telephone (only available with IP Softphone R4 and later)**

  This mode allows you to make and receive calls under the control of the IP Softphone - just like in the **Telecommuter** or **Road Warrior** mode. The big difference is that you have a real digital telephone under your control. In the **Road Warrior** mode, there is no telephone. In the Telecommuter mode, the telephone you are using (whether analog, digital, or IP telephone is brain dead). In this mode (if you have an IP telephone), you get the best of both worlds.

- **Control of DCP Telephone (only available with IP Softphone R5 and later)**

  This feature provides a registration endpoint configuration that will allow an IP softphone and a non-softphone telephone to be in service on the same extension at the same time. In this new configuration, the call control is done by both the softphone and the telephone endpoint. The audio is done by the telephone endpoint.

Tip:

Use status station to show the part (product) ID, serial number, and the audio connection method used by existing stations.

Note:

Beginning with the November 2003 release of Communication Manager, R1 and R2 IP Softphone and IP Agent, which use a dual connect (two extensions) architecture, are no longer supported. R3 and R4 IP Softphone and IP Agent, which use a single connect (one extension) architecture, continue to be supported. This applies to the RoadWarrior and the Telecommuter configurations for the IP Softphone. Native H.323 registrations for R1 and R2 Softphones continue to be supported.

Enabling the system to use IP softphone

Procedure

1. Display the System Parameters Customer-Options (Optional Features) screen.
2. Verify the following field settings:
   - **Maximum Concurrently Registered IP Stations** is greater than 0.
   - **IP Stations** field is y
   - Information has been entered in the fields on the Maximum IP Registrations by Product ID page
3. Verify that your DEFINITY CSI has a CLAN board and an IP Media Processor board.
4. Install the IP Softphone software on each IP Softphone user’s PC.

Road Warrior Mode

You can use the road-warrior mode when you have only a single telephone line available to access Avaya Communication Manager over the IP network.

You also can “take over” an IP telephone. Typically you would not have a different extension for your softphone. When you log in, the softphone takes over the existing telephone extension (turn the DCP or IP telephone off). During this time, that DCP or IP telephone is out of service. This is accomplished if, on the Station screen, the **IP Softphone** field is y.

We will add a road-warrior mode at extension 3001. Except for single-connect IP telephones, you have to actually administer two extensions for each road-warrior mode.

Adding a Road Warrior mode

Procedure

1. Type `add station 3000`.
2. Press `Enter`.
   The Station screen appears.
3. In the **Type** field, enter `H.323`.
4. Press `Enter` to save your work.

Administering Road Warrior

Procedure

1. Type `add station next`.
2. Press `Enter`.
   The Station screen appears.

   ✱ **Note:**

   You choose to change an existing DCP extension by using `change station nnnn` in this step, where nnnn is the existing DCP extension.
3. In the **Type** field, enter the model of telephone you want to use.
   For example, enter `6408D`.
4. In the **Port** field, type `x` for virtual telephone or enter the port number if there is hardware.

   ✱ **Note:**

   Port 1720 is turned off by default to minimize denial of service situations. This applies to all IP softphones release 5.2 or later. You can change this setting, if you have root privileges on the system, by typing the command: `/opt/ecs/sbin ACL 1720 on` or `off`.
5. In the **Security Code** field, enter the password for this remote user.
   For example, enter `1234321`.

   This password can be 3-8 digits in length.
6. In the **Media Complex Ext** field, type `3000`.

   This is the H.323 extension just administered.
7. In the **IP Softphone** field, type `y`.
8. On page 2, in the **Service Link Mode** field, type `as-needed`.

   Set this field to `permanent` only for extremely busy remote telephone users, such as call center agents.
9. In the **Multimedia Mode** field, type `enhanced`.
10. Press `Enter` to save your work.

    Now you can install and configure the software on the user's PC. In this example, the user will login by entering their DCP extension (3001) and password (1234321).

Adding a telecommuter mode

About this task

Assign this configuration to remote users who have two available telephone lines. For example, the following steps show how to administer a telecommuter mode for a home user at extension 3010.

Procedure

1. Type `add station 3010`.
2. Press `Enter`.
   The Station screen appears.

   Note:

   Use the `add station` command if this is a new DCP extension. Use the `change station` command for an existing DCP extension and ignore steps 3 and 4.)
3. In the **Port** field, type `x` for virtual telephone or enter the port number if there is hardware.
4. In the **Security Code** field, enter the password for this remote user.
   For example, enter `1234321`.

   This password can be up to 7 digits in length.
5. In the **IP Softphone** field, type `y`.
6. On page 2, in the **Service Link Mode** field, type `as-needed`.

   Set this field to permanent only for extremely busy remote telephone users, such as call center agents.
7. In the **Multimedia Mode** field, type `enhanced`.
8. Press `Enter` to save your work.

   Now you can install and configure the software on the user's PC. In this example, the user will login by entering their DCP extension (3010) and password (1234321).

Troubleshooting IP Softphones

Problem

Display characters on the telephone can not be recognized.

Possible Causes

Microsoft Windows is not set to use Eurofont characters.

Proposed solution

Procedure

1. Set the Microsoft Windows operating system to use Eurofont.
2. Refer to user documentation on the Avaya IP Softphone for more information on how to install and configure the IP Softphone software.

IP Telephones

The 4600-series IP Telephones are physical sets that connect to Avaya Communication Manager via TCP/IP.

⚠ **Caution:**

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. Please be advised that an Avaya IP endpoint cannot dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. You should not use an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations.

Adding an IP telephone

Before you begin

Verify the system has a:

- TN2302 IP Media Processor circuit pack for audio capability
- TN799 Control-LAN circuit pack for signaling capability (for CSI Servers only)

Be sure that your system has been enabled to use IP Telephones. Display the System-Parameters Customer-Options (Optional Features) screen and verify the following field settings.

- **Maximum Concurrently Registered IP Stations** is greater than 0
- **IP Stations** field is y
- Information has been entered in the fields on the Maximum IP Registrations by Product ID page.

About this task

These steps show how to add an IP telephone at extension 4005 and how to assign an extension.

Procedure

1. Type `add station 4005`.
2. Press `Enter`.
   The Station screen appears.

   > ✱ **Note:**
   >
   > When adding a new 4601 or 4602 IP telephone, you must use the 4601+ or 4602+ station type. This station type enables the Automatic Callback feature. When making a change to an existing 4601 or 4602, you receive a warning message, stating that you should upgrade to the 4601+ or 4602+ station type in order to access the Automatic Callback feature.

   The **Port** field is display-only, and IP appears
3. In the **Security Code** field, enter the password for the IP telephone user.

   Although the system accepts a null password, the IP telephone will not work unless you assign a password.
4. Press `Enter` to save your work.

Changing from dual-connect to single-connect IP telephones

About this task

When you have a dual extension telephone and you upgrade to a single extension telephone, you can remove the connection that is no longer used for that telephone. To remove the H.323 connection that is no longer needed, first record the media complex extension number:

Procedure

1. Type `change station nnnn` where nnnn is the extension number of the original dual-connect telephone that you are replacing with a single-connect telephone.

The Station screen appears.

2. Move to the **Media Complex Extension** field.
3. Write down the number in the **Media Complex** field, then delete the number from the field.
4. Press `Enter` to save your work.
5. Remove the extension you recorded. Before you remove an H.323 extension from your system, check the status, remove it from any group or usage lists, and then delete it from the system's memory.
   For example, if you wrote down extension 1234 before you removed it from the **Media Complex** field on the Station screen, then remove extension 1234 using these steps:
6. Type `status station 1234`.
7. Press `Enter`.
   The General Status screen appears.
8. Make sure that the extension is idle (not making or receiving calls), has no messages waiting and has no active buttons (such as **Send All Calls** or **Call Forwarding**)
9. Type `list groups-of-extension 1234`.
10. Press `Enter`.
    The Extension Group Membership screen shows whether the extension is a member of any groups on the system.
11. Press `Cancel`.
12. If the extension belongs to a group, access the group screen and delete the extension from that group.
    If extension 1234 belongs to pickup group 2, type `change pickup group 2` and delete the extension from the list.
13. Type `list usage extension 1234`
14. Press `Enter`.
    The Usage screen shows where the extension is used in the system.
15. Press `Cancel`.
16. If the extension appears on the Usage screen, access the appropriate feature screen and delete the extension.
    If extension 1234 belongs to hunt group 2, type `change hunt group 2` and delete the extension from the list.
17. Type `change station 1234`
18. Press `Enter`.
19. Delete any bridged appearances or personal abbreviated dialing entries

20. Press `Enter`.
    The system displays the Station screen for this telephone so you can verify that you are removing the correct telephone.
21. Type `remove station 1234`.
22. Press `Enter`.
23. If this is the correct telephone, press `Enter`.
    - The system responds with `command successfully completed`.
    - If the system responds with an error message, the telephone is busy or still belongs to a group.
24. Press `Cancel` to stop the request, correct the problem, and type `remove station 1234` again.
25. Remove the extension from voice mail service if the extension has a voice mailbox.
26. Type `save translations`.
27. Press `Enter` to save your changes.

    Note:

    You do not need to delete the extension from coverage paths. The system automatically adjusts coverage paths to eliminate the extension

    Once you successfully remove the extension, it is permanently erased from system memory. If you want to reactivate the extension, you have to add it again as though it were new.

Setting up emergency calls on IP telephones

About this task

Set up which “calling number” to send to the public safety access point when an emergency call is placed from an IP telephone

You use the Station screen to set up emergency call handling options for IP telephones. As an example, we’ll administer the option that prevents emergency calls from an IP telephone.

Procedure

1. Type `change station nnnn` where nnnn is the extension of the telephone you want to modify.
2. Press `Enter`.
   The Station screen appears.

3. Click `Next Page` to find the **Remote Softphone Emergency calls** field.
4. Type `block` in the **Remote Softphone Emergency calls** field.
5. Press `Enter` to save your changes.

> ⚠ **Caution:**
>
> An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. Please be advised that an Avaya IP endpoint cannot dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. You should not use an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones.

Remote office setup

Avaya Remote Office provides IP processing capabilities to traditional call handling for voice and data between Avaya Communication Manager and offices with Remote Office hardware. You need to add the information about Remote Office as a node in Communication Manager, add its extensions, and set up the trunk and signaling groups.

Adding Remote Office to Communication Manager

Before you begin

Be sure the following fields on the System Parameters Customer-Options (Optional Features) screen are set to y or completed. If not, contact your Avaya representative.

- **Maximum Administered Remote Office Trunks**
- **Maximum Administered Remote Office Stations**
- **Product ID registration limit**
- **Remote Office**
- **IP station**
- **ISDN-PRI**

Also, be sure your Remote Office hardware is installed and administered at the remote location. You need the following information from the remote administration:

- IP address
- Password

About this task

In our example, we will set up a remote-office location using Avaya R300 Remote Office Communicator hardware in our branch office in Santa Fe. We will add a new node, and set up the signaling group and trunk group.

Procedure

1. Type `change node-names IP`.
2. Press `Enter`.
   The Node Name screen appears.
3. In the **Name** field, type in a word to identify the node.
   Type `Remote 6`.
4. In the IP address field, type in the IP address to match the one on the Avaya R300 administration.
5. Press `Enter` to save your changes.
6. Type `add remote office` and the number for this remote office.
7. Press `Enter`.
   The Remote Office screen appears.
8. Fill in the following fields
   - **Node Name** - match the name on the IP Node Names screen.
   - **Network Region** - this must match the network region on the IP Interfaces screen for the circuit packs that connect this remote office. Use display ip-interfaces to find this information.
   - **Location** - match the one set up on the Location screen for this remote office.
   - **Site Data** - identify the street address or identifier you want to use.
9. Press `Enter` to save your changes.

   Tip:

   Use status remote office to verify that your server running Communication Manager recognizes the Remote Office information. It also displays the extensions and signaling group you administer next.

Setting up a trunk group

About this task

You can modify an existing trunk group or add a new one. In our example, we will add trunk group 6. Before you start, perform Setting up a signaling group on page 152.

Procedure

1. Type `add trunk group 6`.
   The Trunk Group screen appears.
2. In the **Group Type** field, type `ISDN`.

   ISDN-PRI or ISDN-BRI must be y on the System Parameters Customer-Options (Optional Features) screen.
3. In the **TAC** field, type in the trunk access code that conforms to your dial plan.
4. In the **Carrier Medium** field, type `H.323` (Medpro).
5. In the **Dial Access** field, type `y`.
6. In the **Service Type** field, type `tie`.
7. In the **Signaling Group** field, type in the signaling group you created.
8. Press `Enter` to save your changes.

Setting up a signaling group

About this task

Each Remote Office has its own listen port and signaling group. Set up a new trunk group, or use an existing trunk group administered for H.323 signaling. To set up the signaling group for remote office:

Procedure

1. Type `add signaling-group` and the number of the group you want to add.
   The Signaling Group screen appears.
2. In the **Group Type** field, type `H.323`
3. In the **Remote Office** field, type `y`.
4. In the **Trunk Group for Channel Selection** field, type the number of the trunk you set up for the remote office.

5. In the **Near-end Node Name** field, identify the node name assigned to the CLAN that supports the R300.
6. In the **Far-end Node Name** field, identify the node name assigned to the CLAN that supports the R300.
7. In the **Near-end Listen Port** field, type a port number in the 5000-9999 range.
8. In the **Far-end Listen Port** field, type `1720`.
9. In the **RRQ** field, type `y`.
10. Tab to the **Direct IP-IP Audio Connection** field on another page of this screen and type `y`.
11. Press `Enter` to save your changes.

Setting up Remote Office on network regions

About this task

Now we will set up a network region and show the connections between regions. We begin with network region 1.

Procedure

1. Type `add ip-network-region 1`.
2. Press `Enter`.
   The IP Network Region screen appears.
3. In the **Name** field, describe the region you are setting up
4. In the **Code Set** field, type the codec set you want to use in this region
5. In the **UDP Port Range** field, type the range of the UDP port number to be used for audio transport.
6. In the **Intra-region IP-IP Direct Audio** field, type `y`
7. In the **Inter-region IP-IP Direct Audio** field, type `y`.
8. Move to page 3 to set up connections between regions and assign codecs for inter-region connections.

   Note:

   Page 2 of the IP Network Region screen shows a list of Survivable Remote Server for the network region, and pages 4 through 19 are duplicates of page 3 , providing the ability to administer upto 250 locations.

   The following connections are administered in this example.

- codec-set 2 is used between region 1 and region 4
- codec-set 5 is used between region 1 and region 99
- codec-set 6 is used between region 1 and region 193

9. Assign the region number to the CLAN circuit pack. All the endpoints registered with a specific CLAN circuit pack belong to the CLAN's region.

   See *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504, for more information.

Adding telephones to Remote Office

Before you begin

Be sure the extensions you add fit your dialing plan.

Procedure

1. Type `add station nnnn`, where nnnn is the extension you are adding.
2. Press `Enter`.
   The Station screen appears.
3. In the **Type** field, type in the model of the telephone you are adding.
4. In the **Port** field, type `x`.

   This indicates that there is no hardware associated with the port assignment.
5. In the **Name** field, identify the telephone for your records.
6. In the **Security Code** field, match the password set up on the Remote Office administration.
7. In the **Remote Office Phone** field, type `y`.
8. Press `Enter` to save your changes.

Updating files in the 2410, 2420, 1408, and 1416 DCP telephones

You can copy updated application code into Communication Manager using TFTP over a TCP/IP connection. This eliminates the need to physically remove the telephone and send it to the factory for the firmware update. This feature is available on all of the servers running Avaya Communication Manager.

To allow additional language support for the 1408 and 1416 DCP telephones, the font and language files are available for download. You can visit the Avaya Support site or contact Avaya representative for more information.

Preinstallation tasks for firmware download

Procedure

1. Type `change node-name ip` .
2. Press `Enter`.
   The IP Node Names screen appears.
3. Administer the TFTP server node name and the local node name (CLAN) and IP address.
4. Press `Enter` to save your changes.
5. Type `change ip-interfaces`.
6. Press `Enter`.
   The IP Interfaces screen appears
7. Administer the CLAN Ethernet interface or processor CLAN.
8. Press `Enter` to save your changes.

Downloading the firmware file to Communication Manager

Procedure

1. Place the file on the TFTP server using TFTP, FTP, HTTP or another file transfer program .
2. From the **Web Interface** menu, click the **Set LAN Security** link.
3. Click `Advanced`.
   A list of settings that can be enabled or disabled through the use of check boxes appears.
4. Scroll to **tftp** and check the box enabling inbound tftp traffic.
5. Click `Submit`.
6. Log into SAT and enter `change tftp-server`.
7. Press `Enter`.
   The TFTP Server Configuration screen appears.

8. In theLocal Node Name field, enter the valid local node name from the IP Node Names screen.

   The node must be assigned to a CLAN ip-interface or procr (processor CLAN).
9. In the **TFTP Server Node Name** field, enter the valid TFTP server node name from the IP Nodes Names. screen
10. In the **TFTP Server Port** field, enter the TFTP server port number from where the file download begins.
11. In the **File to Retrieve** field, enter the name of the file to be retrieved.
12. Press `Enter` to save your changes.
    The file transfer begins.
13. Type `display tftp-server`.
14. Press `Enter` to view the status of the file transfer.
    `A File download successful`
    message appears when the file transfer completes. It also displays the file size and the file name in memory.

    After the file is successfully loaded the "Station Type:" will also identify the type of file, either firmware, font, or language, and the phone type the file can be downloaded into which is the 2410, 2420, or 1408/1416. The 1408 and 1416 share common firmware and font/language files.

Downloading firmware to a single station

Before you begin

You must have console permissions to download someone else’s telephones.

Note:

Steps 1 through 5 need be done only once to set up the FAC for file downloads. Thereafter, start at step 6 to download files.

Only one FAC download can be active at a time.

A FAC download cannot be started if a scheduled download is active.

The firmware file and type that is display via the "display tftp" form must be compatible with the station you are downloading.

The target extension must be administered as one of the DCP station types that support firmware download.

Set up a FAC for file downloads

Procedure

1. Type `change feature-access-codes`.
2. Press `Enter`.
3. Click `Next Page` until you see the **Station Firmware Download Access Code** field on the Feature Access Code (FAC) screen.
4. In the **Station Firmware Download Access Code** field, enter a valid FAC as defined in the dial plan.
5. Press `Enter` to save your changes.
6. Take the 2410, 2420, 1408, or 1416 DCP telephone off-hook.
7. Dial the Station Firmware Download FAC.
   For instance, *36.
8. Press `#` if you are dialing from the target station (or dial the telephone's extension to be downloaded).
9. Place the telephone on-hook within 4 seconds after the confirmation tone.
   The telephone is placed in a busy-out state (not able to make or receive calls) and displays `Firmware Download in Progress`, the amount of the file downloaded, and a timer. The telephone displays error messages and a success message before rebooting.

   When the download completes, the telephone reboots and is released from the busy-out state.

Downloading firmware to multiple stations

About this task

You can download firmware to multiple stations of the same type, either 2410, 2420, 1408, or 1416 DCP telephone. Download firmware to as many as 1000 stations per download schedule. You can schedule a specific time for the download, or you can administer the download to run immediately. To download 2410, 2420, 1408, or 1416 DCP station firmware to multiple stations:

Procedure

1. Type `change firmware station-download`.
2. Press `Enter`.
   The Firmware Station Download screen appears.
3. In the **Schedule Download** field, type `y`.
   The **Start Date/Time** and **Stop Date/Time** fields appear.

4. In the **Start Date/Time** field, enter the month (mm), day (dd), year (yyyy), and time (hh:mm) that you want the download to begin.
5. In the **Stop Date/Time** field, enter the month (mm), day (dd), year (yyyy), and time (hh:mm) that you want the download to begin.
6. In the **Continue Daily Until Completed** field, enter `y` if you want the system to execute the firmware download each day at the scheduled time until all specified telephones have received the firmware.
7. In the **Beginning Station** field, enter the first extension number in the range of telephones to which you want to download the firmware.

   Up to 1000 stations can be included in a scheduled download.
8. In the **Ending Station** field, enter the last extension number in the range of telephones to which you want to download firmware.

   Up to 1000 stations can be included in a scheduled download.

   > **Note:**
   >
   > Although you can specify a range of up to 1000 extensions, all 1000 stations are not downloaded simultaneously because there is a limit of how many concurrent phones will be downloaded on a board, gateway, and port network. These limits will likely result in multiple "passes" required to attempt a download to the phone. Also note that on the first "pass" that only two phones will be attempted and if multiple phones fail then the schedule may stop.
9. Press `Enter`.

   The firmware download is set to run at the scheduled time. If you entered `n` in the **Schedule Download?** field, pressing `Enter` immediately initiates the download to the specified range of telephones.

Displaying firmware download status

About this task

You can use the `status firmware download` command to display status information for an active download schedule. To display download status:

Procedure

1. Type `status firmware download`.

   The Status Firmware Station Download screen appears.
2. Press `Enter`.

Note:

If you add the qualifier last to the **`status firmware download`** command, status information on the last download schedule is displayed.

Disabling firmware downloads

About this task

You can use the `disable firmware download` command to disable any active download schedule. To disable active downloads:

Procedure

Type `disable firmware download`.

This command disables any active download schedule and the system displays

```
Command successfully completed
```

at the bottom of the screen.

Native Support of Avaya 1408 and 1416 digital telephones

Native support of Avaya 1408 (1400 Mid) and 1416 (1400 High) digital telephones is available from Communication Manager 6.0 and later. Communication Manager supports call processing features for the Avaya 14xx digital telephones just like Avaya 24xx digital telephones, along with support for the following:

- Fixed feature buttons (Hold, Conference, Transfer, Message waiting lamp, Drop and Redial)
- Message button
- 40 Unicode, Eurofont, or Kanafont character display message support
- Speakerphone functionality (including Group Listen)
- Eight call appearances or feature buttons

Note:

To allow firmware upgrades and to utilize the new capabilities of the sets, the phone type must be administered as either 1408 or 1416.

Native Support of Avaya 1408 digital telephone

Communication Manager provides native administration for the Avaya 1408 digital telephone. The Avaya 1408 digital telephone administration is similar to the Avaya 2410 digital telephone with the same fields and default values except for the following:

- Support for eight call appearances or feature buttons
- No **Customizable Labels** field
- No **Media Complex Ext** field
- Support for display languages which include English, Spanish, French, Italian, User defined, Unicode, Unicode2, Unicode3, and Unicode4

Native Support of Avaya 1416 digital telephone

Communication Manager provides native administration for the Avaya 1416 digital telephone. The Avaya 1416 digital telephone administration is similar to the Avaya 2420 digital telephone with the same fields and default values except for the following:

- Support for 16 call appearances or feature buttons
- No **Customizable Labels** field
- No **Data Option** field
- No **Media Complex Ext** field
- Support for display languages which include English, Spanish, French, Italian, User defined, Unicode, Unicode2, Unicode3, and Unicode4
- Support for **Button Modules** field rather than **Expansion Module** field

BM32 Button Support

The Avaya 1416 digital telephone uses the BM32 button expansion module. Communication Manager supports two BM32 buttons for the Avaya 1416 digital telephone.

Administer location per station

Use the Administer location per station feature to:

- Allow IP telephones and softphones connected through a VPN to be associated with the branch that an employee is assigned to.
- Allow a VPN connected employee to have the same dialing experience as others in the office who are connected through a gateway.

Related topics:

Preparing to administer location number on Station screen on page 161
Setting up location number on Station screen on page 161

Preparing to administer location number on Station screen

Procedure

On the Optional Features screen, ensure that the **Multiple Locations** field is set to `y`. If this field is set to `n`, your system is not enabled for the Administer location per station feature. Contact your Avaya representative for assistance.

✱ **Note:**

If the **Multiple Locations** field on the Optional Features screen is set to `n`, the **Location** field on the Station screen is hidden.

To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

For a complete description of the many Optional Features screens, see Administering Avaya Aura™ Communication Manager, 03-300509.

Setting up location number on Station screen

Procedure

1. Enter `change station` *`n`*, where *n* is the extension number to which you want to assign a location.
2. In the **Location** field, enter a valid location number.

   This field appears only when the **Type** field is set to H.323 or SIP.
3. Select `Enter` to save your changes.

   ✱ **Note:**

   If the station extension is a SIP telephone type and if the application type is OPS on the Stations with Off-PBX Telephone Integration screen, then the Off-PBX screen's **Location** field is display-only and displays the value of the **Location** field of the corresponding Station screen.

Chapter 7: Telephone Features

Once you add a telephone to the system, you can use the Station screen to change the settings for the telephone, such as adding or changing feature button assignments. The system allows you to assign features or functionality to each programmable button. It is up to you to decide which features you want for each telephone and which feature you want to assign to each button. If you have 6400-series telephones, your users can administer some of their own feature buttons. See *Setting up Terminal Self-Administration* for more information.

✱ **Note:**

An NI-BRI telephone with Communication Manager has only the **Conference**, **Transfer**, **Hold**, and **Drop** feature buttons, none of which requires administration. On an NI-BRI telephone, you can assign additional feature buttons only as call appearances. As a result, NI-BRI telephone users must access all other features of Communication Manager using feature access codes. Additionally, the number of call appearance buttons administered in Communication Manager (the default is three) must match the number of call appearances programmed on the telephone. Finally, Communication Manager does not support bridged call appearances for NI-BRI telephones.

Adding feature buttons

Procedure

1. Type `change station nnnn` where nnnn is the extension for the telephone you want to modify.
2. Press `Enter` .
3. Press `Next Page` until you locate the **Button Assignment** section of the Station screen.

   Some telephones have several feature button groups. Make sure that you are changing the correct button. If you do not know which button on the telephone maps to which button-assignment field, see your telephone’s manual, or see *Telephone Reference*.
4. Enter the button name that corresponds to the feature you want to assign a feature button. To determine feature button names, press Help, or refer to *Telephone Feature Buttons Table*.

   ✱ **Note:**

   For certain newer telephones with expanded text label display capabilities, you can customize feature button labels to accept up to 13 alphanumeric characters.

For more information about this feature, see *Increasing Text Fields for Feature Buttons*.

5. Press `Enter` to save your changes.

   Some telephones have default assignments for buttons. For example, the 8411D includes defaults for 12 softkey buttons. It already has assignments for features like Leave Word Calling and Call Forwarding. If you do not use an alias, you can easily assign different features to these buttons if you have different needs. If you use an alias you must leave the default softkey button assignments. The system allows you to change the button assignments on the screen and the features work on the alias telephone, however the labels on the display do not change.

Related topics:

Increasing Text Fields for Feature Buttons on page 164
Telephone Feature Buttons Table on page 166

Increasing Text Fields for Feature Buttons

If you are using certain newer phones with expanded text label display capabilities, the Increase Text Fields for Feature Buttons feature allows you to program and store up to 13 character labels for associated feature buttons and call appearances. This feature is available for the following telephones:

- 2410 (Release 2 or newer)
- 2420 (Release 4 or newer)
- 4610 (IP Telephone Release 2.2 or later)
- 4620 (IP Telephone Release 2.2 or later)
- 4621 (IP Telephone Release 2.2 or later)
- 4622 (IP Telephone Release 2.2 or later)
- 4625 (IP Telephone Release 3.1 or later)

Related topics:

Adding feature buttons on page 163
Telephone Feature Buttons Table on page 166

Enabling extended text fields for feature buttons

About this task

To enable extended text fields for feature buttons:

Procedure

1. Type `add station next` or `change station nnnn`, where nnnn is the extension of the telephone you want to customize feature button labels for.
   The Station screen appears.
2. Ensure that **Customizable Labels** is set to `y`.

   This allows the user to enter 13-character labels for all feature buttons and call appearances associated with this station.
3. Press `Enter` to save your changes
4. Assign specific feature buttons as described in *Adding Feature Buttons*.

   Note:

   You can also use the existing Abbreviated Dialing (AD) button type (Abr Program) to program AD labels. However, if you choose to utilize the Abr Program button to program AD labels, you are limited to 5 upper case characters. For more information on Abbreviated Dialing, see *Adding Abbreviated Dialing Lists* .

Restricting customization of feature button types

About this task

In order to manage the usage of your system's allocation of customized button labels to ensure that VIP users have the button label customization resource available to them, you can restrict button label customization of up to 50 specified button types for users who are not considered to be VIP users. To restrict customization of specific feature button types:

Procedure

1. Type `change button-restriction` .
   The Button Type Customization Restrictions screen appears.
2. Ensure that **Restrict Customization Of Button Types** is set to `y`.
3. In the fields under Restrict Customization Of Labels For The Following Button Types, enter the button type you want to restrict users from customizing.

Note:

When you enter the special button types abr-spchar or abrv-dial, an additional field appears to the right of the button type as shown in Figure 45. Use this special field to specify the special character associated with the abr-spchar button type or the **Abbreviated Dialing List** associated with the abrv-dial button type.

4. Press `Enter` to save your changes.

Telephone Feature Buttons Table

The following table provides descriptions of the feature buttons that you can administer on multiappearance telephones. It also lists the administrable software names and recommended button label names. **Display** buttons support telephones equipped with alphanumeric displays. Note that some buttons might require 1-lamp or 2-lamp buttons. Some buttons are not allowed on some systems and on some telephones.

Note:

An NI-BRI telephone with Communication Manager has only the **Conference**, **Transfer**, **Hold**, and **Drop** feature buttons, none of which requires administration. On an NI-BRI telephone, you might assign additional feature buttons only as call appearances. As a result, NI-BRI telephone users must access all other features of Communication Manager using feature access codes.

Additionally, the number of call appearance buttons administered in Communication Manager (the default is three) must match the number of call appearances programmed on the telephone.

Finally, Communication Manager does not support bridged call appearances for NI-BRI telephones.

Table 2: Telephone Feature Buttons

Button Name	Button Label	Description	Maximum
#	AD	You can administer the # button as an autodial feature button by entering the Audix number in the **BUTTON ASSIGNMENTS** field on the Station screen.	1 per station
abr-prog	Abr Program	Abbreviated Dialing Program: allows users to program abbreviated dialing and autodial buttons or to store or change numbers in a personal list or group list associated with the station	1 per station

Button Name	Button Label	Description	Maximum
abr-spchar	AbrvDial (char)	Abbreviated Dialing Special Character: allows users to enter an associated special character [~, ~m (mark), ~p (pause), ~s (suppress), ~w (wait for dial tone), or ~W (wait forever)] when programming	1 each per station
abrdg-appr (Ext: _____)	(extension)	Bridged Appearance of an analog telephone: allows the user to have an appearance of a single-line telephone extension. Assign to a 2-lamp appearance button.	Depends on station type
abrv-dial (List: __ DC: __)	AD	Abbreviated Dialing: dials the stored number on the specified abbreviated dialing list. List: specify the list number 1 to 3 where the destination number is stored DC: specify the dial code for the destination number	1 per AD list per dial code
abrv-ring	AbRng	Abbreviated and Delayed Ringing: allows the user to trigger an abbreviated or delayed transition for calls alerting at an extension	
ac-alarm	AC Alarm	Administered Connection alarm notification: allows the user to monitor when the number of failures for an administered connection has met the specified threshold.	1 per station
aca-halt	Auto-Ckt Halt	Automatic Circuit Assurance (display button): allows users of display telephones to identify trunk malfunctions. The system automatically initiates a referral call to the telephone when a possible failure occurs. When the user presses ACA Halt, the system turns off ACA monitoring for the entire system. The user must press ACA Halt again to restart monitoring	1 per system
account	Account	Account: allows users to enter Call Detail Recording (CDR) account codes. CDR account codes allow the system to associate and track calls according to a particular project or account number.	1 per station
admin	Admin	Administration: allows a user to program the feature buttons on their 6400-series telephone.	1 per station
after-call Grp:___	AfterCall	After Call Work Mode: allows an agent to temporarily be removed from call distribution in order for the agent to finish ACD-related activities such as completing paperwork. Grp: specify the ACD split group number.	1 per split group

Button Name	Button Label	Description	Maximum
alrt-agchg	Alert Agent	Alert Agent: indicates to the agent that their split/skill hunt group changed while active on a call. This button blinks to notify the agent of the change.	1 per station
alt-frl	Alternate FRL	Alternate Facility Restriction Level (FRL): activates or deactivates an alternate facility restriction level for the extension.	1 per system
ani-requst	ANI Request	Automatic Number Identification Request: allows the user to display the calling party's number from incoming trunks during the voice state of call. The trunk must support this functionality.	1 per station
assist (Group: __)	Assist	Supervisory Assistance: used by an ACD agent to place a call to a split supervisor. Group: specify the ACD split group number.	1 per split group
asvn-halt	ASVN Halt	Authorization Code Security Violation Notification: activates or deactivates call referral when an authorization code security violation is detected.	1 per system
atd-qcalls	AttQueueCal l	Attendant Queue Calls (display button): tracks the number of calls in the attendant group's queue and displays the queue status. Assign this button to any user who you want to backup the attendant.	1 per station
atd-qtime	AttQueueTim e	Attendant Queue Time (display button): tracks the calls in the attendant group's queue according to the oldest time a call has been queued, and obtains a display of the queue status.	1 per station
audix-rec	Audix Record	Audix One-Step Recording (display button): activates/deactivates recording of the current call. An Audix hunt group extension that is valid for the user must be entered in the Ext: field after the name.	1 per station
aut-msg-wt (Ext: ___)	Msg (name or ext #)	Automatic Message Waiting: associated status lamp automatically lights when an LWC message has been stored in the system for the associated extension (can be a VDN). This lamp will not light on the mapped-to physical station for messages left for virtual extensions.	1 per aut-mst-ex t
auto-cback	Auto CallBack	Automatic Call Back: when activated, allows inside user who placed a call to a busy or	1 per station

Button Name	Button Label	Description	Maximum
		unanswered telephone to be called back automatically when the called telephone becomes available to receive a call.	
auto-icom (Group: __)	Autoic (name or ext #)	Automatic Intercom: places a call to the station associated with the button. The called user receives a unique alerting signal, and a status lamp associated with a Intercom button flashes. Grp: Intercom — Auto-Icom group number. This extension and destination extension must be in the same group.	1 per group per dial code
auto-in (Group: __)	Auto in	Auto-In Mode: allows the user to become automatically available for new ACD calls upon completion of an ACD call. Grp: The split group number for ACD.	1 per split group
auto-wkup	Auto Wakeup	Automatic Wakeup (display button): allows attendants, front-desk users, and guests to request a wakeup call to be placed automatically to a certain extension (cannot be a VDN extension) at a later time.	1 per station
autodial	SD	Allows a user to dial a number that is not part of a stored list.	
aux-work (RC: __) (Group: __)	AuxWork	Auxiliary Work Mode: removes agent from ACD call distribution in order to complete non-ACD-related activities. RC: Optional assignment for the 1- or 2-digit Reason Code to be used to change to Aux Work using this button, when Reason Codes is active. Multiple Aux Work buttons, each with a different RC, can be assigned to the same station set. Grp: The split group number for ACD.	1 per split group
brdg-appr (Btn: __ Ext: ___)	(extension)	Bridged Call Appearance: provides an appearance of another user's extension on this telephone. For example, an assistant might have a bridged appearance of their supervisor's extension. The bridged appearance button functions exactly like the original call appearance, for instance it indicates when the appearance is active or ringing. You can assign brdg-appr buttons only to 2-lamp appearance buttons. You must indicate which extension and which call	Depends on station type

Button Name	Button Label	Description	Maximum
		appearance button the user wants to monitor at this telephone.	
btn-ring	Button Ring	Station User Button Ring Control: allows users to toggle between audible and silent call alerting.	1 per station
btn-view	Button View	Button View: allows users to view, on the telephone's display, the contents of any feature button. Button View does more than the "View" or "stored-num" feature button; these only display what is contained in abbreviated dialing and autodial buttons. When the user presses the btn-view button and then a specific feature button, they see the feature name and any auxiliary data for that button. This allows users to review the programming of their feature buttons. You can assign this soft-key button to any 6400-, 7400-, or 8400-series display telephone.	
busy-ind (TAC/Ext: __)	Busy	Busy Indication: indicates the busy or idle status of an extension, trunk group, terminating extension group (TEG), hunt group, or loudspeaker paging zone. Users can press the busy-ind button to dial the specified extension. You can assign this button to any lamp button and must specify which Trunk or extension the user wants to monitor.	1 per TAC/ Ext
call-appr	extension	Call Appearance: originates or receives calls. Assign to a 2-lamp appearance button.	Depends on station type
call-disp	Return Call	Call Displayed Number (display button): initiates a call to the currently displayed number. The number can be from a leave word calling message or a number the user retrieved from the Directory.	1 per station
call-fwd (Ext: ___)	CFrwd (Ext #) Call Forward (no ext #)	Activates or deactivates Call Forwarding All Calls.	64 per extension
call-park	Call Park	Allows the user to place the current call in the call park state so it can be retrieved from another telephone.	1 per station
call-pkup	Call Pickup	Allows the user to answer a call that is ringing in the user's pickup group.	1 per station

Button Name	Button Label	Description	Maximum
call-timer	Call Timer	Used only on the 6400 sets. Allows users to view the duration of the call associated with the active call appearance button	1 per station
call-unpk	Unpark Call	Allows the user to unpark a call from another telephone than the telephone that originally parked the call. This feature button applies only to the SIP station types.	1 per station
callr-info	Caller Info	(display button) Used with Call Prompting to allow users to display information collected from the originator.	1 per station
cas-backup	CAS Backup	Centralized Attendant Service Backup: used to redirect all CAS calls to a backup extension in the local branch if all RLTs are out-of-service or maintenance busy. The associated status lamp indicates if CAS is in the backup mode.	1 per station
cdr1-alrm	CDR 1 Fail	CDR Alarm: associated status lamp is used to indicate that a failure in the interface to the primary CDR output device has occurred.	1 per station
cdr2-alrm	CDR 2 Fail	CDR Alarm: associated status lamp is used to indicate that a failure in the interface to the secondary CDR output device has occurred.	1 per station
cfwd-bsyda	CFBDA	Call Forward Busy/Don't Answer: activates and deactivates call forwarding for calls when the extension is busy or the user does not answer.	64 per extension
cfwd-enh	ECFwd (ext #) Enhanced Cfwd (no ext #)	Call Forwarding - Enhanced allows the user to specify the destination extension for both internal and external calls.	
check-in	Check In	Check In (display button): changes the state of the associated guest room to occupied and turns off the outward calling restriction for the guest room's station.	1 per station
check-out	Check Out	Check Out (display button): Changes the state of the associated guest room to vacant and turns on the outward calling restriction for the guest room's station. Also clears (removes) any wake-up request for the station.	1 per station

Button Name	Button Label	Description	Maximum
clk-overid	ClkOverride	Clocked Manual Override (display button): Used only by authorized attendants and system administrators, in association with Time of Day Routing, to override the routing plan in effect for the system. The override is in effect for a specified period of time. This feature can only be assigned to display telephones.	1 per station
conf-dsp	Conf Display	Allows a user to display information about each party of a conference call. This button can be assigned to stations and attendant consoles.	1 per station
consult	Consult	The Consult button allows a covering user, after answering a coverage call, to call the principal (called party) for private consultation. Activating Consult places the caller on hold and establishes a private connection between the principal and the covering user. The covering user can then add the caller to the conversation, transfer the call to the principal, or return to the caller.	1 per station
cov-cback	CovrCallBac k	Allows a covering party to store a leave word calling message for the principal (called party).	1 per station
cov-msg-rt	Covr Msg Ret	Coverage Message Retrieval (display button): places a covering station into the message retrieval mode for the purposes of retrieving messages for the group.	1 per station
cpn-blk	CPN Block	Blocks the sending of the calling party number for a call.	1 per station
cpn-unblk	CPN Unblock	Deactivates calling party number (CPN) blocking and allows the CPN to be sent for a single call.	1 per station
crss-alert	Crisis Alert	Crisis Alert (display button): provide this button to the telephones or consoles that you want to notify when any user makes an emergency call. (You define which calls are emergency calls on the AAR/ARS Analysis screen by setting the Call Type to alrt.) After a user receives an alert, they can press the crss-alert button to disable the current alert. If tenant partitioning is active, the attendants within a partition can receive emergency	1 per station 10 per system

Button Name	Button Label	Description	Maximum
		notification only from callers in the same partition.	
data-ext	Data (data ext #)	Data Extension: sets up a data call. Can be used to pre-indicate a data call or to disconnect a data call. Cannot be a VDN or ISDN-BRI extension.	1 per data extension group
date-time	Time/Date	Date and Time (display button): displays the current date and time. Do not assign this button to 6400-series display telephones as they normally show the date and time.	1 per station
delete-msg	Delete Msg	Delete message (display button): deletes a stored LWC message or wakeup request.	1 per station
dial-icom (Grp: ___)	Dial Icom	Dial Intercom: accesses the intercom group assigned to the button. Grp: Intercom — Dial (Dial Icom) group number.	1 per group
did-remove	DID Remove	DID Remove (display button): allows DID assignments to be removed.	1 per station
did-view	DID View	DID View (display button): allows DID assignments to be displayed and changed. Allows choice between XDID and XDIDVIP numbers	1 per station
directory	Directory	Directory (display button): allows users with display telephones to access the integrated directory, use the touch-tone buttons to key in a name, and retrieve an extension from the directory. The directory contains the names and extensions that you have assigned to the telephones administered in your system. If you assign a directory button, you should also assign a Next and Call-Disp button to the telephone. These buttons allow the user to navigate within the integrated directory and call an extension once they find the correct one. **Note:** Vector Directory Numbers do not appear in the integrated directory. Also, if you assign a name beginning with two tildes (~~} to a telephone, and Display Character Set on the System Parameters Country-Options screen is set to Roman, the name does not appear in the integrated	1 per station

Button Name	Button Label	Description	Maximum
		directory. Note that this is the only way to hide a name in the integrated directory.	
dir-pkup	Dir Pickup	Directed call pickup: allows the user to answer a call ringing at another extension without having to be a member of a pickup group.	
disp-chrg	Disp Charges	Provides your display telephone with a visual display of accumulated charges on your current telephone call. Used exclusively outside the U.S. and Canada.	1 per station
disp-norm	Local/ Normal	Normal (display button): Toggles between LOCAL display mode (displays time and date) and NORMAL mode (displays call-related data). LED off = LOCAL mode and LED on = NORMAL.	1 per station
dn-dst	DoNotDisturb	Places the user in the do not disturb mode.	1 per station
drop	Drop	Allows users to drop calls. Users can drop calls from automatic hold or drop the last party they added to a conference call.	
ec500	EC500	Administers an Extension to Cellular feature button on the office telephone. When you enter this value, the Timer subfield displays, and defaults to n. Set the optional **Timer** subfield to y to include an Extension to Cellular timer state for the administered feature button. When the timer state is included, the Extension to Cellular user can activate a one-hour timer to temporarily disable Extension to Cellular through this administered feature button. Leaving the default setting of n excludes the timer state	1 per station
exclusion	Exclusion	Exclusion: allows multiappearance telephone users to keep other users with appearances of the same extension from bridging onto an existing call. If the user presses the Exclusion button while other users are already bridged onto the call, the other users are dropped. There are two means of activating exclusion.	1 per station

Button Name	Button Label	Description	Maximum
		• Manual Exclusion — when the user presses the Exclusion button (either before dialing or during the call). • Automatic Exclusion — as soon as the user picks up the handset. To turn off Automatic Exclusion during a call, the user presses the Exclusion button. To use Automatic Exclusion, set the **Automatic Exclusion by COS** field to `y` on the Feature-Related System Parameters screen.	
ext-dn-dst	ExtDoNotDisturb	Extension — Do Not Disturb (display button): used by the attendant console or hotel front desk display telephone to activate do not disturb and assign a corresponding deactivate time to an extension.	1 per station
ext-pkup	Call Pickup Extended	Allows the user to answer calls directly from another call pickup group. This feature button applies only to the SIP station types.	1 per station
extnd-call	Extend Call	Allows the user to extend the current call to an Off-PBX/EC500 telephone	1 per station
fe-mute	fe-mute Far End Mute	Allows a user to mute a selected party on a conference call. This button can be assigned to stations and attendant consoles.	1 per station
flash	Flash	1) Allows a station on a trunk call with Trunk Flash to send a Trunk Flash signal to the far end (e.g., Central Office); 2) allows a station on a CAS main call to send a Trunk Flash signal over the connected RLT trunk back to the branch to conference or transfer the call.	1 per station
goto-cover	Goto Cover	Go To Coverage: sends a call directly to coverage instead of waiting for the called inside-user to answer. Go to Cover forces intercom and priority calls to follow a coverage path. **Note:** Go to Cover cannot be activated for calls placed to a Vector Directory Number extension. Go to Cover can be used to force a call to cover to a VDN if the called principal has a VDN as a coverage point.	1 per station

Button Name	Button Label	Description	Maximum
grp-dn-dst	GrpDoNotDstrb	Group Do Not Disturb (display button): places a group of telephones into the do not disturb mode.	1 per station
grp-page (Number:___)	GrpPg	Allows users to make announcements to groups of stations by automatically turning on their speakerphones. Number: The extension of the page group.	
headset	Headset	Signals onhook/offhook state changes to Communication Manager. The green LED is on for offhook state and off (dark) for onhook state.	1 per station
hunt-ns (Grp: ___)	HuntNS	Hunt-Group Night Service: places a hunt-group into night service. Grp: Hunt group number.	3 per hunt group
in-call-id (Type: __ Grp: ___)	INCallID (group #, type, name, or ext #)	The Coverage Incoming Call Identification (ICI) button allows a member of a coverage answer group or hunt group to identify an incoming call to that group even though the member does not have a display telephone. In the Type field, enter c for coverage answer groups and type of h for a hunt group. In the Grp field, enter the group number.	1 per group-type per group
inspect	Inspect	Inspect (display button): allows users on an active call to display the identification of an incoming call. Inspect also allows users to determine the identification of calls they placed on Hold.	1 per station
Inst-trans	Instant Transfer	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.	1 per station
int-aut-an	IntAutoAnswer	Internal Automatic Answer: causes any hybrid or digital station to automatically answer incoming internal calls.	1 per station
last-numb	LastNumb Dialed	Last Number Dialed (redial): originates a call to the number last dialed by the station.	1 per station

Button Name	Button Label	Description	Maximum
lic-error	License Error	License-Error: indicates a major License File alarm. Pressing the button does not make the light go out. The button goes out only after the error is cleared and Communication Manager returns to License-Normal Mode. You can administer this button on telephones and attendant consoles.	1 per telephone 20 per system (Server CSI)
limit-call	LimitInCalls	Limit Number of Concurrent Calls feature: allows user to limit the number of concurrent calls at a station to one call, where normally multiple call appearances can terminate at the station.	1 per station
link-alarm (link# ___)	Link Fail (link #)	Link Alarm: associated status lamp indicates that a failure has occurred on one of the Processor Interface circuit pack data links. Link: Link number — 1 to 8 for multi-carrier cabinets or 1 to 4 for single-carrier cabinets.	8 per station
lsvn-halt	LSVN Halt	Login Security Violation Notification: activates or deactivates referral call when a login security violation is detected.	1 per system
lwc-cancel	Cancel LWC	Leave Word Calling Cancel: cancels the last leave word calling message originated by the user.	1 per station
lwc-lock	Lock LWC	Leave Word Calling Lock: locks the message retrieval capability of the display module on the station.	1 per station
lwc-store	Store LWC	Leave Word Calling Store: leaves a message for the user associated with the last number dialed to return the call to the originator.	1 per station
major-alrm	Major Alarm	Major Alarm: assign to a status lamp to notify the user when major alarms occur. Major alarms usually require immediate attention.	1 per station
man-msg-wt (Ext: ___)	Msg Wait (name or ext #)	Manual Message Waiting: allows a multiappearance telephone user to press a button on their telephone in order to light the Manual Message Waiting button at another telephone. You can administer this feature only to pairs of telephones, such as an assistant and an executive. For example, an assistant can press the man-msg-wt button to signal the executive that they have a call.	None
man-overid (TOD: _)	ManOverid	Immediate Manual Override (display button): allows the user (on a system with Time of Day	1 per station

Button Name	Button Label	Description	Maximum
		Routing) to temporarily override the routing plan and use the specified TOD routing plan. TOD: specify the routing plan the user wants to follow in override situations.	
manual-in (Group: __)	Manual In	Manual-In Mode: prevents the user from becoming available for new ACD calls upon completion of an ACD call by automatically placing the agent in the after call work mode. Grp: The split group number for ACD.	1 per split group
mct-act	MCT Activate	Malicious Call Trace Activation: sends a message to the MCT control extensions that the user wants to trace a malicious call. MCT activation also starts recording the call, if your system has a MCT voice recorder.	1 per station
mct-contr	MCT Control	Malicious Call Trace Control: allows the user to take control of a malicious call trace request. Once the user becomes the MCT controller, the system stops notifying other MCT control extensions of the MCT request. NOTE: To add an extension to the MCT control group, you must also add the extension on the Extensions Administered to have an MCT-Control Button screen. When the user presses the MCT Control button, the system first displays the called party information. Pressing the button again displays the rest of the trace information. The MCT controller must dial the MCT Deactivate feature access code to release control.	1 per station
mf-da-intl	Directory Assistance	Multifrequency Operator International: allows users to call Directory Assistance.	1 per station
mf-op-intl	CO attendant	Multifrequency Operator International: allows users to make international calls to the CO attendant.	1 per station
mj/mn-alrm	Mj/Mn Alarm	Minor Alarm: assign to a status lamp to notify the user when minor or major alarms occur. Minor alarms usually indicate that only a few trunks or a few stations are affected.	1 per station
mm-basic	MM Basic	Multimedia Basic: used to place a multimedia complex into the "Basic" mode or to return it to the "Enhanced" mode	1 per station
mm-call	MM Call	Multimedia Call: used to indicate a call is to be a multimedia call.	1 per station

Button Name	Button Label	Description	Maximum
mm-cfwd	MM Call Fwd	Multimedia Call Forward: used to activate forwarding of multimedia calls as multimedia calls, not as voice calls.	1 per station
mm-datacnf	MM Data Cnf	Multimedia Data Conference: used to initiate a data collaboration session between multimedia endpoints; requires a button with a lamp.	1 per station
mm-multnbr	MM Mult Nbr	Indicate that the user wants to place calls to 2 different addresses using the 2 B-channels.	1 per station
mm-pcaudio	MM PC Audio	Switches the audio path from the telephone (handset or speakerphone) to the PC (headset or speakers/ microphone).	1 per station
msg-retr	Msg Retrieve	Message Retrieval (display button): places the station's display into the message retrieval mode.	1 per station
mwn-act	MsgWaitAct	Message Waiting Activation: lights a message waiting lamp on an associated station.	1 per station
mwn-deact	MsgWaitDeact	Message Waiting Deactivation: dims a message waiting lamp on an associated station.	1 per station
next	Next	Next (display button): steps to the next message when the telephone's display is in Message Retrieval or Coverage Message Retrieval mode. Shows the next name when the telephone's display is in the Directory mode.	1 per station
night-serv	Night Service	Night Service Activation: toggles the system in or out of Night Service mode.	1 per station
noans-alrt	NoAnsAlrt	Redirection on No Answer Alert: indicates a Redirection on No Answer timeout has occurred for the split.	1 per hunt group
no-hld-cnf	No Hold Conf	No Hold Conference: can automatically conference another party while continuing the existing call.	1 per station
normal	Normal	Normal (display button): places the station's display into normal call identification mode.	1 per station
off-bd-alm	OffBoardAlarm	Off board Alarm: associated status lamp lights if an off-circuit pack major, minor, or warning alarm is active on a circuit pack. Off-	1 per attendant

Button Name	Button Label	Description	Maximum
		board alarms (loss of signal, slips, misframes) relate to problems on the facility side of the DS1, ATM, or other interface.	
per-COline (Grp: ___)	COLine (line #)	Personal CO Line: allows the user to receive calls directly via a specific trunk. Grp: CO line group number.	1 per group
pms-alarm	PMS Failure	Property Management System alarm: associated status lamp indicates that a failure in the PMS link occurred. A major or minor alarm condition raises the alarm.	1 per station
post-msgs	Posted MSGs	Posted Messages: Allows the user to display a specific message to callers.	1 per station
pr-awu-alm	pr-awu-alm AutoWakeAlarm	Automatic Wakeup Printer Alarm: associated status lamp indicates that an automatic wakeup printer interface failure occurred.	1 per station
pr-pms-alm	PMS Ptr Alarm	PMS Printer Alarm: associated status lamp indicates that a PMS printer interface failure occurred.	1 per station
pr-sys-alm	Sys Ptr Alarm	System Printer Alarm: associated status lamp indicates that a system printer failure occurred.	1 per station
print-msgs	Print Msgs	Print Messages: allows users to print messages for any extension by pressing the button and entering the extension and a security code.	1 per station
priority	Priority Call	Priority Calling: allows a user to place priority calls or change an existing call to a priority call.	1 per station
q-calls (Grp: ___)	QueueCall	Queue Calls: associated status lamp flashes if a call warning threshold has been reached. Grp: Group number of hunt group.	1 per hunt group per station
q-time (Grp: ___)	QueueTime	Queue Time: associated status lamp flashes if a time warning threshold has been reached. Grp: Group number of hunt group.	1 per hunt group per station
release	Release	Releases an agent from an ACD call.	1 per station
ring-stat	Ringer Status	Users can display the ringer status for a line or bridged appearance by pressing the ring-stat button followed by a call-appr, brdg-appr or abrdg-appr button. Depending on the ringer status, the display shows	1 per station

Button Name	Button Label	Description	Maximum
		• Ringer On • Ringer Off • Ringer Delayed • Ringer Abbreviated	
ringer-off	Ringer Off	Ringer-Cutoff: silences the alerting ringer on the station.	1 per station
rs-alert	ResetAlert	The associated status lamp lights if a problem escalates beyond a warm start.	1 per station
rsvn-halt	RSVN Halt	Remote Access Barrier Code Security Violation Notification Call: activates or deactivates call referral when a remote access barrier code security violation is detected.	1 per station
scroll	Scroll	Scroll (display button): allows the user to select one of the two lines (alternates with each press) of the 16-character LCD display. Only one line displays at a time.	1 per station
send-calls (Ext: ___)	SAC (ext #)	Send All Calls allows users to temporarily direct all incoming calls to coverage regardless of the assigned call-coverage redirection criteria. Assign to a lamp button.	64 per extension
send-term	Send TEG	Send All Calls For Terminating Extension Group: allows the user to forward all calls directed to a terminating extension group.	1 per TEG
serv-obsrv	Service Obsrv	Service Observing: activates Service Observing. Used to toggle between a listen-only and a listen-talk mode.	1 per station
share-talk	Share Talk	Share Talk: enables multiple DCP or H323 IP endpoints that are registered to the same extension to share talk capability. Normally, when more than one endpoint requests RTP (Real Time Transfer Protocol) media, only one of the endpoints (Base Set) is capable of talking and listening, while the other endpoints are connected in listen-only mode. This button allows all the endpoints that are associated with the extension to share the talk capability. Note that in Communication Manager 5.0, only AE Server DMCC (Device, Media, and Call Control) endpoints are capable of requesting RTP while they are	1 per station

Button Name	Button Label	Description	Maximum
		sharing control of the extension. For more information on DMCC, see *Avaya MultiVantage® Application Enablement Services Administration and Maintenance Guide, 02-300357.*	
signal (Ext: ___)	Sgnl (name or ext #)	Signal: allows the user to use one button to manually signal the associated extension. The extension cannot be a VDN extension.	1 per signal extension
ssvn-halt	SSVN Halt	Toggle whether or not station security code violation referrals are made to the referral destination.	1 per station
sta-lock	Station Lock	When Station Lock is enabled, the only calls that can be made from the station are those allowed by the COR administered in the Station Lock COR field.	1 per station
start-bill	Start Bill	After an ACD agent answers a call, the agent can press this button to send an ISDN CONNECT message to the PSTN network to start the PSTN call–billing for a call at the PSTN switch.	1 per station
stored-num	Stored Number	Enables a display mode that displays the numbers stored in buttons.	1 per station
stroke-cnt (Code:_)	Stroke Count (#)	Automatic Call Distribution Stroke Count # (0, 1, 2, 3, 4, 5, 6, 7, 8, or 9) sends a message to CMS to increment a stroke count number.	Upto 10 per station
team	Team	The Team Button has two generic functions, a display function and an execution function. The display function allows any member of a team (monitoring station) to observe the station state of other team members (monitored station). As an execution function, the Team Button can be used as Speed Dial Button or Pick-Up Button where a call to the monitored station is established directly or a ringing call is picked from the monitored station. Ext: This field appears when you enter the button type team. Enter the extension of the principal station of the virtual "team." Rg This field appears when you enter the button type team. Enter the kind of audible ringing for the team button. Valid entries are a(bbreviated), d(elayed), n(o-ring), and r(ing).	15 per monitoring station

Button Name	Button Label	Description	Maximum
term-x-gr (Grp: ___)	TermGroup (name or ext #)	Terminating Extension Group: provides one or more extensions. Calls can be received but not originated with this button. Grp: TEG number.	1 per TEG
timer	Timer	Used only on the 6400 sets. Allows users to view the duration of the call associated with the active call appearance button	1 per station
togle-swap	Toggle-Swap	Allows a user to toggle between two parties before completing a conference or a transfer	1 per station
trk-ac-alm	FTC Alarm	Facility Test Call Alarm: associated status lamp lights when a successful Facility Test Call (FTC) occurs.	1 per station
trk-id	Trunk ID	Trunk Identification (display button): identifies the tac (trunk access code) and trunk member number associated with a call.	1 per station
trunk-name	Trunk Name	(display button) Displays the name of the trunk as administered on the CAS Main or on a server without CAS.	1 per station
trunk-ns (Grp: ___)	Trunk NS	Trunk-Group Night Service: places a trunk-group into night service. Grp: Trunk group number.	3 per trunk group
usr-addbsy	Add Busy Indicator	Adds the busy indicator.	1 per station
usr-rembsy	Remove Busy Indicator	Removes the busy indicator.	1 per station
uui-info	UUI-Info	Allows users to see up to 32 bytes of ASAI-related UUI-IE data.	1 per station
verify	Verify	Busy Verification: allows users to make test calls and verify a station or a trunk.	1 per station
vip-chkin	VIP Check In	VIP Check-in (display button): allows user to assign the XDIDVIP number to the room extension.	1 per station
vip-retry	VIP Retry	VIP Retry: starts to flash when the user places a VIP wakeup call and continues to flash until the call is answered. If the VIP wakeup call is not answered, the user can press the VIP Retry button to drop the call and reschedule the VIP wakeup call as a classic wakeup call. To assign this button,	1 per station

Button Name	Button Label	Description	Maximum
		you must have both Hospitality and VIP Wakeup enabled.	
vip-wakeup	VIP Wakeup	VIP Wakeup: flashes when a VIP wakeup reminder call is generated. The user presses the button to place a priority (VIP) wakeup call to a guest. To assign this button, you must have both Hospitality and VIP Wakeup enabled.	1 per station
voa-repeat	VOA Repeat	VDN of Origin Announcement. VDN of Origin Announcement must be enabled.	1 per station
voice-mail	Message	This is not an administrable button, but maps to the fixed hard "message" button on newer telephones.	1 per station
vu-display (format: __ ID: __)	Vu Display #	VuStats Display: allows the agent to specify a display format for the statistics. If you assign a different VuStats display format to each button, the agent can use the buttons to access different statistics. You can assign this button only to display telephones. format: specify the number of the format you want the button to display ID (optional): specify a split number, trunk group number, agent extension, or VDN extension	limited to the number of feature buttons on the telephone
whisp-act	whisp-act WhisperAct	Whisper Page Activation: allows a user to make and receive whisper pages. A whisper page is an announcement sent to another extension who is active on a call where only the person on the extension hears the announcement; any other parties on the call cannot hear the announcement. The user must have a class of restriction (COR) that allows intra-switch calling to use whisper paging.	1 per station
whisp-anbk	WhisperAnb k	Whisper Page Answerback: allows a user who received a whisper page to respond to the user who sent the page.	1 per station
whisp-off	WhisperOff	Deactivate Whisper Paging: blocks other users from sending whisper pages to this telephone.	1 per station
work-code	Work Code	Call Work Code: allows an ACD agent after pressing "work-code" to send up to 16 digits (using the dial pad) to CMS.	1 per station

Related topics:

Adding feature buttons on page 163

Increasing Text Fields for Feature Buttons on page 164

Abbreviated Dialing Lists

Abbreviated dialing is sometimes called speed dialing. It allows you to dial a short code in place of an extension or telephone number. When you dial abbreviated-dialing codes or press abbreviated-dialing buttons, you access stored numbers from special lists. These lists can be personal (a list of numbers for an individual telephone), group (a department-wide list), system (a system-wide list), or enhanced numbers (allows for a longer list of numbers). The version and type of your system determine which lists are available and how many entries you can have on each list.

Note:

You can designate all group-number lists, system-number lists, and enhanced-number lists as "privileged." Calls automatically dialed from a privileged list are completed without class of restriction (COR) or facility restriction level (FRL) checking. This allows access to selected numbers that some telephone users might otherwise be restricted from manually dialing. For example, a user might be restricted from making long-distance calls. However, you can program the number of a branch office that is long distance into an AD list as privileged. Then, the user can call this office location using AD, while still being restricted from making other long-distance calls.

Security alert:

Privileged group-number, system-number, and enhanced-number lists provide access to numbers that typically would be restricted.

Setting up a station to access a new group list

About this task

We will set up station 4567 so it has access to the new group list

Procedure

1. Type `change station 4567`.
2. Press `Enter`.
3. Press `Next Page` until you see Station screen (page 4), containing the **Abbreviated Dialing List** fields.
4. Type `group` in any of the **List** fields.

5. Press `Enter`.
   A blank **list number** field appears.
6. Type `3` in the **list number** field.

   When you assign a group or personal list, you must also specify the personal list number or group list number.
7. Press `Enter` to save your changes.

   The user at extension 4567 can now use this list by dialing the feature access code for the list and the dial code for the number they want to dial. Alternatively, you can assign an abbreviated dialing button to this station that allows the user press one button to dial a specific stored number on one of their three assigned abbreviated lists.

Adding Abbreviated Dialing Lists

About this task

You can program a new group list.

Procedure

1. Type `add abbreviated-dialing group next` .
2. Press `Enter`.
   The Abbreviated Dialing List screen appears. In our example, the next available group list is group 3.
3. Enter a number (in multiples of 5) in the **Size** field.

   This number defines the number of entries on your dialing list.

   if you have 8 telephone numbers you want to store in the list, type 10 in the **Size** field.
4. If you want another user to be able to add numbers to this list, enter their extension in the **Program Ext** field.
   If you want the user at 4567 to be able to change group list 3, enter `4567` in this field
5. Enter the telephone numbers you want to store, one for each dial code.

   Each telephone number can be up to 24 digits long.
6. Press `Enter` to save your changes.

   You can display your new abbreviated-dialing list to verify that the information is correct or print a copy of the list for your paper records. Once you define a group list, you need to define which stations can use the list.

Troubleshooting abbreviated dialing lists

Dial list connects to wrong number

Problem

A user complains that using an abbreviated dial list dials the wrong number.

Possible Causes

- The user entered an wrong dial code.
- The dial code was wrongly defined.

Proposed solution

Procedure

1. Ask the user what number they dialed or button they pressed to determine which list and dial code they attempted to call.
2. Access the dialing list and verify that the number stored for the specific dial code corresponds to the number the user wanted to dial.
   To access a group list, type display abbreviated-dialing group x, press `Enter`, where x is a group list number
3. If the user dialed the wrong code, give them the correct code.
4. If the dial code is wrong, press `Cancel` and use the appropriate change command to re-access the abbreviated dialing list.
5. Correct the number.
6. Press `Enter`.

Cannot access dial list

Problem

A user cannot access a dial list

Possible Causes

- The specific list was not assigned to the user's telephone.
- The user dialed the wrong feature access code
- The user pressed the wrong feature button.
- The feature button was wrongly defined.

Proposed solution–Verify list assigned to telephone

Procedure

1. Type `display station nnnn`, where nnnn is the user’s extension.
2. Press `Enter`.
3. Review the current settings of the **List1** , **List2** , and **List3** fields to determine if the list the user wants to access is assigned to their telephone.

Proposed solution–Verify feature access code

Procedure

1. Type `display feature-access-codes`.
2. Press `Enter`.
3. Verify that the user is dialing the appropriate feature access code.

Proposed solution–Verify feature button assignment

Procedure

1. Type `display station nnnn`, where nnnn is the user’s extension.
2. Press `Enter`.
3. Review the current feature button assignments to determine whether:
   - The user was pressing the assigned button.
   - The list number and dial code are correct.

Abbreviated Dialing Lists-Limitations

There are limits to the total number of abbreviated dialing list entries, the number of personal dial lists, and the number of group dial lists that your system can store. Because of these limitations, you should avoid storing the same number in more than one list. Instead, assign commonly dialed numbers to the system list or to a group list. You can determine the abbreviated dialing storage capacity, by referring to the System Capacity screen for the abbreviated dialing values (type display capacity). For details on the System Capacity screen, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

Bridged Call Appearances

Think of a bridged call appearance as a telephone (the primary set) with an extension (the bridged-to appearance). Both telephones can be used to call in and out and both show when a line is in use. A call to the primary telephone is bridged to a specific appearance, or button, on the secondary telephone. The secondary telephone retains all its functions, and a specific button is dedicated as the bridged-to appearance from the primary telephone. Bridged call appearances have to be assigned to telephones with double-lamp buttons, or lights. The telephone types do not need to match, but as much consistency as possible is recommended for all telephones in a bridged group. When a call comes in on bridged telephones, the buttons assigned to the bridged appearances flash. You can assign as many bridged appearances as there are line appearances on the primary telephone, and you can assign ringing (alerting) to one or more of the telephones.

Setting Up Bridged Call Appearances

About this task

Create a bridged call appearance.

Procedure

1. Note the extension of the primary telephone .

   A call to this telephone lights the button and, if activated, rings at the bridged-to appearance on the secondary telephone.
2. If you want to use a new telephone for the bridged-to extension, duplicate a station.
3. Type `change station and the bridged-to extension`.
4. Press `Enter`.
5. Press `Next Page` until the **Feature Options** page of the Station screen appears
6. For the **Per Button Ring Control** field (digital sets only):
   - If you want to assign ringing separately to each bridged appearance, type `y`.
   - If you want all bridged appearances to either ring or not ring, leave the default `n`.
7. Move to Bridge Call Alerting.
8. If you want the bridged appearance to ring when a call arrives at the primary telephone, type `y`. Otherwise, leave the default `n`.
9. Complete the appropriate field for your telephone type.

- If your primary telephone is analog, move to the **Line Appearance** field and enter `abrdg-appr`
- If your primary telephone is digital, move to the **BUTTON ASSIGNMENTS** field and enter `brdg-appr`.

10. Press `Enter`.
    Btn and **Ext** fields appear. If **Per Button Ring Control** is set to y on the Station screen for the digital set, **Btn**, **Ext**, and **Ring** fields appear
11. Enter the primary telephone's button number that you want to assign as the bridged call appearance.
    This button flashes when a call arrives at the primary telephone.
12. Enter the primary telephone extension.
13. If the Ring field appears:
    - If you want the bridged appearance to ring when a call arrives at the primary telephone, type `y`.
    - If you do not want the bridged appearance to ring, leave the default `n`.
14. Press `Enter` to save your changes.
15. To see if an extension has any bridged call appearances assigned, type list bridge and the extension.
16. Press `Enter`.
    The user at extension 4567 can now use this list by dialing the feature access code for the list and the dial code for the number they want to dial. Alternatively, you can assign an abbreviated dialing button to this station that allows the user press one button to dial a specific stored number on one of their three assigned abbreviated lists.

When to use Bridged Call Appearances

Following is a list of example situations where you might want to use bridged appearances.

- A secretary making or answering calls on an executive's primary extension: These calls can be placed on hold for later retrieval by the executive, or the executive can simply bridge onto the call. In all cases, the executive handles the call as if he or she had placed or answered the call. It is never necessary to transfer the call to the executive.
- Visitor telephones: An executive might have another telephone in their office that is to be used by visitors. It might be desirable that the visitor be able to bridge onto a call that is active on the executive's primary extension number. A bridged call appearance makes this possible.
- Service environments: It might be necessary that several people be able to handle calls to a particular extension number. For example, several users might be required to answer calls to a hot line number in addition to their normal functions. Each user might also be

required to bridge onto existing hot line calls. A bridged call appearance provides this capability.

- A user frequently using telephones in different locations: A user might not spend all of their time in the same place. For this type of user, it is convenient to have their extension number bridged at several different telephones.

Extension to Cellular

Use the Extension to Cellular feature to extend your office calls and Communication Manager features to a cellular telephone. For a detailed description of the Extension to Cellular feature and how to administer it, see Extension to Cellular in*Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, or *Avaya Extension to Cellular User's Guide*, 210-100-700.

Extension to Cellular Setup Table

The following table provides a quick reference to the screens and fields used in administering the Extension to Cellular feature.

Table 3: Screens for administering Extension to Cellular

Screen Name	Purpose	Fields
Stations with Off-PBX Telephone Integration	Map station extensions to application types and	**All**
Off-PBX Telephone Mobile-Feature-Extension	Administer CTI feature.	**Mobile Call (CTI) Extension**
Feature Access Code (FAC)	Set up access codes for Communication Manager features.	**Feature Access Code**
Extension to Call Which Activate Features by Name	Map a dialed extension to activate a feature (FNE) within Communication Manager from a cell phone. Some FNEs require FAC administration.	**Extension**
Telecommuting Access	Create an Extension to Cellular remote access number.	**All**
Security-Related System Parameters	Define a system-wide station security code length.	**Minimum Station Security Code Length**

Screen Name	Purpose	Fields
Station	Assign feature buttons and timers.	**BUTTON ASSIGNMENTS**
Language Translations	To review the office telephone feature button assignments	**All**
Numbering-Public/ Unknown Format	Assign 10-digit caller identification.	**All**
Coverage Path	Set up number of unanswered rings prior to coverage.	**Number of Rings**
Trunk Group	Enable Call Detail Recording for outgoing trunk.	**CDR Reports**
DS1 Circuit Pack	Administer a DS1 Circuit pack for R2MFC for EC500 use.	**Signaling Mode: CAS** **Interconnect: CO**
Trunk Group	Administer a trunk group for EC500 use. **Note:** For more information, see Extension to Cellular in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.	**Group Type** **Trunk Type** **Outgoing Dial Type** **Incoming Dial Type** **Receive Answer Supervision?**
Multifrequency-signaling-related-parameters	Administer MFC parameters needed for EC500. **Note:** For more information, see Guidelines for administering Multifrequency Signaling in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.	**Incoming Call Type: group-ii-mfc (for MFC signaling)** **Outgoing Call Type: group-ii-mfc (for MFC signaling)** **Request Incoming ANI (non-AR/ARS) y**
System Capacity	Verify used, available, and system station limits.	**Off-PBX Telephone - EC500** **Off-PBX Telephone - OPS** **Off-PBX Telephone - PBFMC** **Off-PBX Telephone - PVFMC**

Setting Up Extension To Cellular Feature Access Button

About this task

Extension to Cellular provides the capability to administer an Extension to Cellular feature access button on the user's office telephone to enable and disable the feature. You can also configure an optional timer. You administer this feature button on page 3 of the Station screen for the "host" office extension to which Extension to Cellular is linked. The process described below explains how to administer an Extension to Cellular feature button and include the optional Extension to Cellular timer. The Extension to Cellular feature button is available on telephones which support administrable feature buttons.

Procedure

1. Type `change station n`, where n is the extension of an Extension to Cellular enabled station
   Type `1034`.
2. Press the `Next Page` button twice to display the Station screen (page 4).
3. Select an available feature button under the `BUTTON ASSIGNMENTS` header (button 4 was used in this example) and type `ec500` to administer an Extension to Cellular feature button on the office telephone.
4. Press `Enter`.

   Note:

   The **Timer** subfield displays, and defaults to n. Leaving the default setting of n excludes the timer state
5. Set the optional **Timer** subfield to `y` to include an Extension to Cellular timer state for the administered feature button

   When the timer state is included, the Extension to Cellular user can activate a one-hour timer to temporarily disable Extension to Cellular through this administered feature button.
6. Press **Enter**.
   The corresponding feature button on the office telephone is now administered for Extension to Cellular.

   Note:

   The feature status button on the office telephone indicates the current state of Extension to Cellular regardless of whether the feature was enabled remotely or directly from the office telephone.

   For additional information, see the *Avaya Extension to Cellular User's Guide, 210-100-700*.

Terminal Self-Administration

Before a user can enter the TSA Admin mode, their telephone must be completely idle. After a user presses the Admin button and enters a security code (if necessary), they are prompted, via the telephone's display, to choose features to administer to buttons on their telephone. The user can add, replace, or delete any of the following feature-button types from their telephone.

- CDR Account Code
- Automatic Dial
- Blank
- Call Forwarding
- Call Park
- Call Pickup
- Directed Call Pickup
- Group Page
- Send All Calls
- Toggle Swap
- Activate Whisper Page
- Answerback for Whisper Page
- Whisper Page Off

End-user button changes are recorded to the Communication Manager server's history log so that remote services can know what translations are changed.

Setting Up Terminal Self-Administration

Before you begin

To prevent users from changing another user's telephone administration, you can enable the system-wide option that requires users to enter a station security code before they can administer their telephone.

To enable this option:

1. Set the **Station Security Code for Terminal Self-Administration Required** on the Security-Related System Parameters screen to `y`.
2. If you enable this option, the user is prompted for the station security code when they press the **Admin** button. The user must enter the security code, followed by the pound (#) button or the **Done** softkey.

About this task

Terminal self-administration (TSA) allows users to administer some of their own feature buttons from their telephones. TSA is available for 6400-series, and 4612 and 4624 telephones. Users are prompted, via the telephone's display, to choose features to assign to buttons on their telephones.

You need to assign a security code to the user's Station screen for each user you want to enable access to TSA. You also need to assign the user an Admin feature button. For example, to assign a security code of 12345678 to extension 4234, complete the following steps:

Procedure

1. Type `change station 4234`,.
2. Press `Enter`.
   The Station screen for extension 4234 appears.
3. In the **Security Code** field, type `12345678`

   You should assign unique security codes for each user. Once you enter the code and move off the field, the system changes the field to '*' for extra security.
4. In one of feature button fields, type `admin`.

   You can assign this button to a feature button or a softkey.
5. Press `Enter` to save your changes.

Fixing Problems in Terminal Self-Administration

Symptom	Cause and Solution
When a telephone is in the Admin mode, the telephone is not able to accept any calls	The telephone is treated as if it were busy. Also, a user cannot make calls while in the Admin mode.
Any button state a telephone is in when the telephone enters the Admin mode stays active while the telephone is in	

Symptom	Cause and Solution
the Admin mode.	
ACD agents who wish access to the Admin mode of TSA must be logged off before pressing the Admin button.	If they are not logged off when they attempt to enter the Admin mode, they receive a denial (single-beep) tone.
Call Forwarding can be active and works correctly in the Admin mode.	An active **Call Forwarding** button cannot be removed when the telephone is in the Admin mode.
The telephone must be on-hook to go into the Admin mode.	The **Headset On/Off** button must be in the OFF position.
A telephone that is in the Admin mode of TSA cannot be remotely unmerged by the PSA feature.	If a user has Abbreviated and Delayed Ringing active, a call can be silently ringing at a telephone and the user might not realize it. This ringing prevents the user from entering the Admin mode of TSA.

Enterprise Mobility User

Enterprise Mobility User (EMU) is a software-only feature that provides the ability to associate the buttons and features of a primary telephone to a telephone of the same type anywhere within your company's enterprise.

A home station can be visited by another EMU user while the user is registered as an EMU visitor elsewhere. A home station can be used as a visited station while the principal user's EC500 or other Off-PBX applications are active. And the principal user can activate an Off-PBX application even if their home station is being visited by another EMU user.

Note:

In this document, any telephone that is not the primary telephone is referred to as the “visited” telephone and any server that is not the home server of the primary telephone is referred to as the “visited server.”

System Requirements — EMU

The following is a list of requirements that you need for the EMU feature:

- QSIG must be the private networking protocol in the network of Communication Manager systems. This requirement also includes QSIG MWI

  Note:

  All systems in a QSIG network must be upgraded to Communication Manager 4.0 or later in order for the Enterprise Mobility User feature to function properly. If only some systems are upgraded, and their extensions expanded, the EMU feature might not work with the systems that have not been upgraded. See your Avaya technical representative for more information
- Communication Manager Release 3.1 or later software must be running on the home server and all visited servers.
- All servers must be on a Linux platform. EMU is not supported on DEFINITY servers.
- The visited telephone must be the same model type as the primary telephone to enable a optimal transfer of the image of the primary telephone. If the visited telephone is not the same model type, only the call appearance (**call-appr**) buttons and the message waiting light are transferred.
- All endpoints must be terminals capable of paperless button label display.
- Uniform Dial Plan (UDP)
- To activate the EMU feature, a user enters the EMU activation feature access code (FAC), the extension number of their primary telephone, and the security code of the primary telephone on the dial pad of a visited telephone. The visited server sends the extension number, the security code, and the set type of the visited telephone to the home server. When the home server receives the information, it:
  - Checks the class of service (COS) for the primary telephone to see if it has PSA permission
  - Compares the security code with the security code on the Station screen for the primary telephone
  - Compares the station type of the visited telephone to the station type of the primary telephone. If both the visited telephone and the primary telephone are of the same type, the home server sends the applicable button appearances to the visited server. If a previous registration exists on the primary telephone, the new registration is accepted and the old registration is deactivated

  If the registration is successful, the visited telephone assumes the primary telephone’s extension number and some specific administered button types. The display on the primary telephone shows **Visited Registration Active: <Extension>:** The extension number that displays is the extension number of the visited telephone

Note:

The speed dialing list that is stored on the primary telephone and the station logs are not downloaded to the visited telephone.

Configuring your System for the Enterprise Mobility User

Procedure

1. Type `display cos` to view your Class of Service settings.
   The system displays the Class of Service screen.
2. Verify that the **Personal Station Access (PSA)** field is set to `y`.

   This field applies to the primary telephone and must be set to y for EMU.
3. Type `display feature-access-codes`.
   The system displays the Feature Access Code (FAC) screen
4. In one of feature button fields, type `admin`.
5. Scroll down until you see the fields for **Enterprise Mobility User Activation and Deactivation**.

   The feature access codes (FACs) for both EMU activation and EMU deactivation must be set on all servers using EMU. You must enter the FAC of the server in the location from which you are dialing.

   Note:

   To avoid confusion, Avaya recommends that all the servers in the network have the same EMU feature access codes.
6. On page 3 of the Feature Related System Parameters screen, use the **EMU Inactivity Interval for Deactivation** (hours) field to administer a system-wide administrable interval for EMU deregistration at a visited switch.
7. Click `Enter` to save your changes.

Setting EMU options for stations

Procedure

1. Enter `add station next`.
2. Enter the security code of your primary telephone when you activate or deactivate EMU. The security code is administered on page one of the Station screen. The

security code can be up to eight numbers. No letters or special characters are allowed. Once the security code is entered, the system displays a * in the **Security Code** field.

3. On the Station screen, scroll down till you find the **EMU Login Allowed** field.

   The **EMU Login Allowed** field applies to the visited station and must be set to y for EMU. The valid entries to this field are y or n, with n as the default. You must set this field to `y` to allow this telephone to be used as a visited station by an EMU user.

4. Select `Enter` to save your changes.

Defining options for calling party identification

Procedure

1. Type `display trunk-group x`, where x is the number of the trunk group.
   The system displays the Trunk Group screen.

2. Scroll down till you see the **Send EMU Visitor CPN** field.

   This field controls calling party identification, that is, the extension of the primary telephone or the extension of the visited telephone that is used when a call is made from a visited telephone.

3. If you want the system to display calling party information of the primary telephone, the **Send EMU Visitor CPN** field must be set to`y` . There are areas where public network trunks disallow a call if the calling party information is invalid. In this case, there can be instances where the extension of the primary telephone is considered invalid and the extension of the visited telephone must be used. To use the extension of the visited telephone, set the **Send EMU Visitor CPN** field to `n`.

   Note:

   If you set the **Send EMU Visitor CPN** field to `y`, you must set the **Format** field on the same page to either public or unk-pvt.

4. Click `Enter` to save your changes.

Activating EMU

Procedure

1. At the visited telephone, enter the EMU activation facility-access-code (FAC).

You must enter the EMU activation FAC of the server in the location where you are dialing from.

2. Enter the extension of your primary telephone set.
3. Enter the security access code of your primary telephone set. This is the security code administered on the primary telephone's station form on the home server.

    - If the registration is successful, you hear confirmation tone.
    - If the registration is not successful, you hear audible intercept.

    Audible intercept is provided when:

    - The registration was rejected by the home server.
    - The telephone where the registration attempt is made is not administered for EMU use.
    - The 15 second timer expires at the visited server.

    If the home server receives a request from a visited server for a telephone that already has an EMU visitor registration active, the old registration is terminated and the new registration is approved. If the primary telephone is in-use when a registration attempt is made, the registration attempt fails.

Deactivating EMU

Procedure

1. At the visited telephone, enter the EMU deactivation FAC.

    You must enter the EMU deactivation FAC of the server in the location where you are dialing from.
2. Enter the extension number of the primary telephone.
3. Enter the security code of the visited telephone.

    If the visited telephone does not deactivate, the telephone remains in the visited state.
4. To deactivate the visited telephone you can perform a busy-out, release busy-out at the visited server.
5. Enter the EMU feature deactivation code and the security code of the visited telephone at the home server location.
6. Press the `<mute>RESET` function on the IP telephone.

    Note:

    Anytime the visited telephone performs a reset, the EMU registration is deactivated.

7. Unplug the visited DCP set for a period of one minute

   Unplugging or disconnecting a 4600 series set will not deactivate the set.

Chapter 8: Managing Attendant Consoles

Attendant Consoles

The attendant console is the main answering position for your organization. The console operator is responsible for answering incoming calls and for efficiently directing or "extending" calls to the appropriate telephone. The attendant console also can allow your attendants to monitor:

- system problems
- toll fraud abuse
- traffic patterns

The number of consoles you can have in your organization varies depending on your Avaya solution.

302 attendant consoles

Avaya Communication Manager supports the following 302 attendant consoles: the 302A/B, 302C, and 302D consoles. You might have a basic or enhanced version of these consoles.

To compare and contrast the consoles, view the diagrams below.

- 302A/B
- 302C
- 302D

302D Console

The 302D console provides the following enhancements to the 302C console:

- Modular handset/headset connection

  The console accepts a standard RJ11, 4-pin modular handset or headset. This connection replaces the quarter-inch, dual-prong handset/headset connection.
- Activate/deactivate push-button

  You can use the push-button on the left side of the console to activate or deactivate the console. A message appears on the console identifying that the button must be pressed to activate the console.
- Two-wire DCP compatibility

The console is compatible with two-wire DCP circuit packs only, not four-wire DCP circuit packs.

- Headset volume control

  The console can now control the volume of an attached headset.

- Noise expander option

  The console has circuitry to help reduce background noise during pauses in speech from the console end of a conversation. This option is normally enabled.

- Support for Eurofont or Katakana character set

  The console can show the Eurofont or Katakana character set. Administration of these character sets must be coordinated with the characters sent from Avaya Communication Manager.

Avaya PC consoles

The Avaya PC Console is a Microsoft Windows-based call handling application for Avaya Communication Manager attendants. It provides an ideal way to increase your productivity and to better serve your customers.

PC Console offers all the call handling capabilities of the hardware-based Avaya 302 attendant console with a DXS module, plus several enhanced features and capabilities. The enhanced features provide you with the ability to see up to six calls at once, and to handle all calls more efficiently.

PC Console also provides a powerful directory feature. You are able to perform searches, display user information, including a photo. You are able to place a call immediately from the directory.

And, because PC Console resides on a Windows-based PC, you are able to use other software applications at the same time. If a call comes in while you are in another application, you are able to handle it immediately.

For more information about the Avaya PC Console, contact your Avaya account team or representative.

SoftConsole IP Attendant

The SoftConsole is a Windows-based application that can replace the 302B hard console. The SoftConsole is similar to PC Console, but it performs call answering and routing through a PC interface via IP. For more information, contact your Avaya account team or representative.

Related topics:

302A/B Console on page 205
302C Console on page 206
302D Console on page 207

302A/B Console

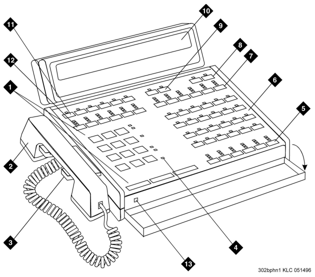


Figure 7: 302A and 302B1 attendant console

Note:

Button numbers map to physical positions on the console.

Figure notes:

1. Call processing area
2. Handset
3. Handset cradle
4. Warning lamps and call waiting lamps
5. Call appearance buttons
6. Feature area
7. Trunk group select buttons
8. Volume control buttons
9. Select buttons
10. Console display panel
11. Display buttons
12. Trunk group select buttons
13. Lamp Test Switch

302C Console

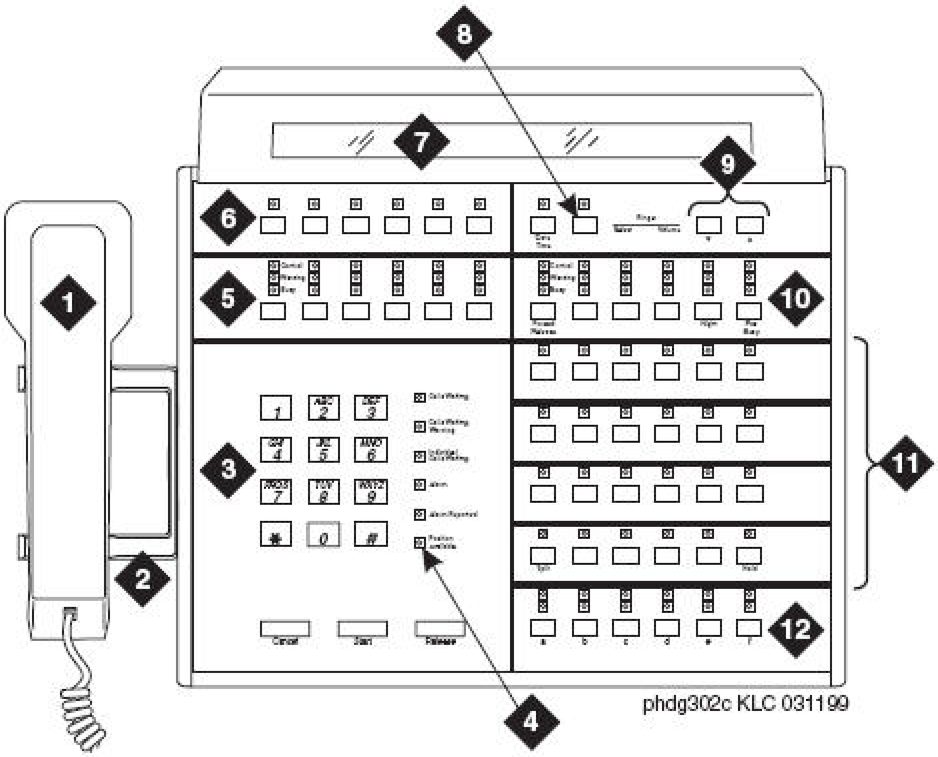


Figure 8: 302C attendant console

Note:

Button numbers map to physical positions on the console.

Figure notes:

1. Handset
2. Handset cradle
3. Call processing area
4. Warning lamps and call waiting lamps
5. Outside-line buttons
6. Display buttons
7. Display
8. Select buttons
9. Volume control buttons

10. Outside-line buttons
11. Feature buttons
12. Call appearance buttons

302D Console

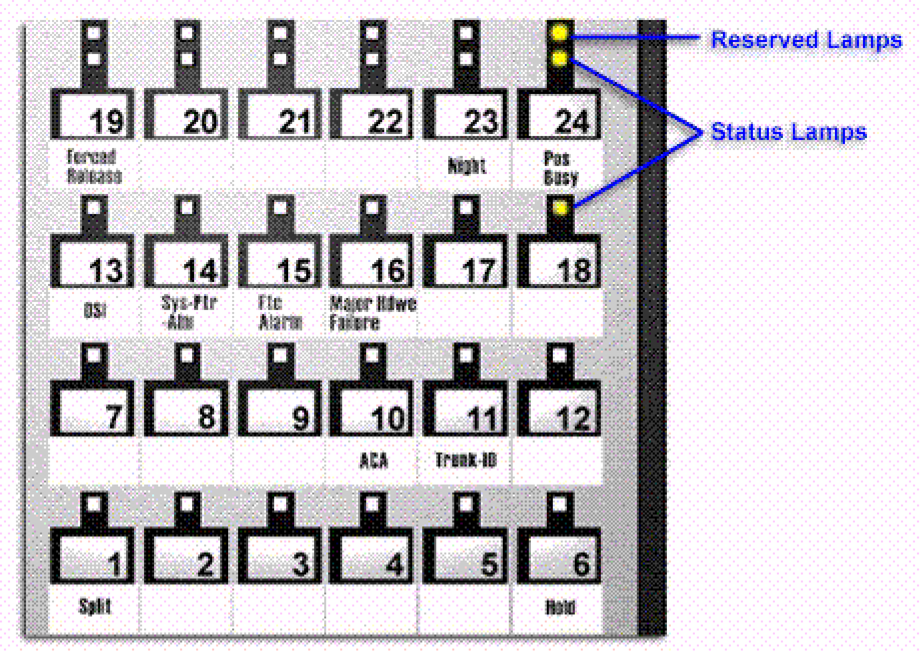


Figure 9: Console feature button layout

Note:

Button numbers map to physical positions on the console.

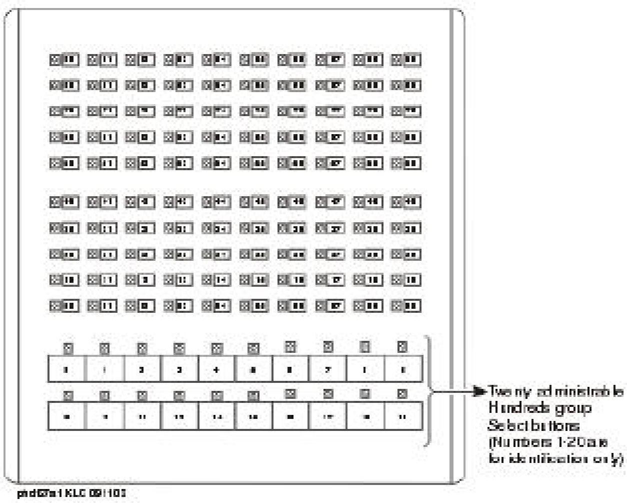


Figure 10: Enhanced Selector Console

Adding an Attendant Console

About this task

Usually Avaya connects and administers your primary attendant console during cutover. However, you might find a need for a second attendant console, such as a backup console that is used only at night. This example shows how to add a night-only attendant console.

Note:

These instructions do not apply to adding a PC Console or SoftConsole. For more information, see the appropriate console documentation.

Procedure

1. Type `add attendant`.
2. Press `Enter`
   The Attendant Console screen appears.
3. In the **Type** field, enter `302`. This is the type of attendant console.
4. If you want this attendant to have its own extension, enter one in the **Extension** field.

   Tip:

   If you assign an extension to the console, the class of restriction (COR) and class of service (COS) that you assign on this Attendant Console screen override the COR and COS you assigned on the Console Parameters screen. To avoid unexpected behavior, you should assign the same COR and same COS on both screens.

If you give your attendants an individual extension, users can call the attendant directly by dialing the extension.

Individual attendant extensions also allow attendants to use features that an attendant group cannot use — for example, you can assign them to hunt groups.

5. In the **Console Type** field, enter `night-only`.

   This indicates how this console is used in your organization—as a principal, day only, night only, or day/night console. You can have only one night-time console (night only or day/ night) in the system.

6. In the **Port** field , enter the port address for this console.
7. Type a name to associate with this console in the **Name** field.
8. In the **DIRECT TRUNK GROUP SELECT BUTTON ASSIGNMENTS** fields, enter trunk access codes for the trunks you want the attendant to be able to select with just one button.
9. If you are using the **Enhanced Selector** console, set the **HUNDREDS SELECT BUTTON ASSIGNMENTS** that you want this console to have.

   If you want this console to be able to access extensions in the range 3500 to 3999, you need to assign them 5 **Hundreds Select Buttons**: 35 for extensions 3500 to 3599, 36, 37, 38, and 39.

10. Assign the Feature Buttons that you want the 302 console to have.

    To determine which buttons you can assign to a console, see *Attendant Console Feature Buttons*.

    Tip:

    Feature buttons are not numbered top-to-bottom on the attendant console, as you might expect.

11. Press **Enter** to save your changes.

Related topics:

Attendant Console Feature Buttons on page 209

Attendant Console Feature Buttons

Feature Buttons

The following table lists the feature buttons that you can assign to an attendant console.

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Note s
Abbreviated Dialing	AD	abrv-dial (List:___ DC:___)	1 per List/ DC	1
Administered Connection [status lamp]	AC Alarm	ac-alarm	1	
Automatic Call Distribution (ACD)	After Call Work	after-call (Grp. No.__)	N	2
	Assist	assist (Grp. No:__)	1 per split group	2
	Auto In	auto-in (Grp. No.__)	1 per split group	2
	Auxiliary Work	aux-work (Grp. No.__)	1 per split group	2
	Manual-In	manual-in (Grp. No.__)	1 per split group	2
	Release	release	1	
	Work Code	work-code	1	
	Stroke (0-9)	stroke-cnt (Code:_)	1	3
Attendant Console (Calls Waiting)	CW Aud Off	cw-ringoff	1	
Attendant Control of Trunk Group Access (Activate)	Cont Act	act-tr-grp	1	
Attendant Control of Trunk Group Access (Deactivate)	Cont Deact	deact-tr-g	1	
Attendant Direct Trunk Group Select	Local TG Remote TG	local-tgs (TAC:__) remote-tgs (LT:__) (RT:__)	12	4
Attendant Crisis Alert	Crisis Alert	crss-alert	1	
Attendant Display [display buttons]	Date/Time	date-time	1	
	Inspect Mode	inspect	1	
	Normal Mode	normal	1	
	Stored Number	stored-num	1	
Attendant Hundreds Group Select	Group Select _	hundrd-sel (Grp:__)	20 per console	5

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Note s
Attendant Room Status	Occupied Rooms Status	occ-rooms	1	6
	Maid Status	maid-stat	1	6
Attendant Override	Override	override	1	
Automatic Circuit Assurance	ACA	aca-halt	1 per system	
Automatic Wakeup (Hospitality)	Auto Wakeup	auto-wkup	1	
Busy Verification	Busy Verify	verify	1	
Call Coverage	Cover Cback	cov-cback	1	
	Consult	consult	1	
	Go To Cover	goto-cover	1	
Call Coverage [display button]	Cover Msg Rt	cov-msg-rt	1	
Call Offer (Intrusion)	Intrusion	intrusion	1	
Call Prompting [display button]	Caller Info	callr-info	1	
Call Type	Call Type	type-disp	1	
Centralized Attendant Service	CAS-Backup	cas-backup	1	
Check In/Out (Hospitality) [display buttons]	Check In	check-in	1	
	Check Out	check-out	1	
Class of Restriction [display button]	COR	class-rstr	1	
Conference Display [display button]	Conference Display	conf-dsp	1	
Demand Print	Print Msgs	print-msgs	1	
DID View	DID View	did-view	1	
Do Not Disturb (Hospitality)	Do Not Disturb	dn-dst	1	
Do Not Disturb (Hospitality) [display buttons]	Do Not Disturb Ext	ext-dn-dst	1	
	Do Not Disturb Grp	grp-dn-dst	1	
Don’t Split	Don’t Split	dont-split	1	

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Note s
Emergency Access To the Attendant	Emerg. Access To Attd	em-acc-att	1	
Facility Busy Indication [status lamp]	Busy (trunk or extension#)	busy-ind (TAC/Ext: _)	1 per TAC/ Ext.	7
Facility Test Calls [status lamp]	FTC Alarm	trk-ac-alm	1	
Far End Mute [display button]	Far End Mute for Conf	fe-mute	1	
Group Display	Group Display	group-disp	1	
Group Select	Group Select	group-sel	1	
Hardware Failure [status lamps]	Major Hdwe Failure	major-alrm	10 per system	
	Auto Wakeup	pr-awu-alm	1	
	DS1 (facility)	ds1-alarm	10 per system	
	PMS Failure	pms-alarm	1	
	PMS Ptr Alm	pr-pms-alm	1	
	CDR 1 Failure	cdr1-alrm	1	
	CDR 2 Failure	cdr2-alrm	1	
	Sys Ptr Alm	pr-sys-alm	1	
Hold	Hold	hold	1	
Integrated Directory [display button]	Integrtd Directory	directory	1	
Incoming Call Identification	Coverage (Group number, type, name, or ext.#)	in-call-id	N	
Intrusion (Call Offer)	Intrusion	intrusion	1	
Leave Word Calling	Cancel LWC	lwc-cancel	1	
	LWC	lwc-store	1	
Leave Word Calling [display buttons]	Delete Msg	delete-msg	1	
	Next	next	1	
	Call Display	call-disp	1	
Leave Word Calling (Remote Message	Msg (name or extension #)	aut-msg-wt (Ext:___)	N	

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Note s
Waiting) [status lamp]				
Link Failure	Link Failure (Link No.__)	link-alarm (Link No.__)	1 per Link #	8
Login Security Violation	lsvn-halt	lsvn-halt	1 per system	
Message Waiting	Message Waiting Act.	mwn-act	1 per system	
	Message Waiting Deact.	mwn-deact	1 per system	
Night Service	Trunk Grp. NS	trunk-ns (Grp. No.__)	1 per trunk group	9
No Answer Alert	noans-altr	noans-altr	1 per group	
Off Board Alarm	off-bd-alm	off-bd-alm	1 per group	
Page 1 Link Alarm Indication	PAGE1 Alarm	pg1-alarm	1 per station	
Page 2 Link Alarm Indication	PAGE2 Alarm	pg2-alarm	1 per station	
PMS Interface [display buttons]	PMS display			
Priority Attendant Group	prio-grp	prio-grp	1	
Priority Calling	Prior Call	priority	N	
Position Busy	Position Busy	pos-busy	1	
Queue Status Indications (ACD) [display buttons]	AQC	atd-qcalls	1	
	AQT	atd-qtime		
Queue Status Indications (ACD) [status lamps]	NQC	q-calls (Grp:_)	1	10
	OQT	q-time Grp:_)	1 per hunt group	10
Remote Access Security Violation	rsvn-halt	rsvn-halt	1 per system	
Ringing	In Aud Off	in-ringoff	1	
Security Violation Notification Halt	ssvn-halt	ssvn-halt	1 per system	
Serial Call	Serial Call	serial-cal	1	

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Note s
Split/Swap	Split-swap	split-swap	1	11
System Reset Alert	System Reset Alert [status lamp]	rs-alert	1	
Station Security Code Notification Halt	ssvn-halt	ssvn-halt	1 per system	
Night Service (ACD)	Hunt Group	hunt-ns (Grp. No.__)	3 per hunt group	12
Time of Day Routing [display buttons]	Immediate Override	man-ovrid	1	
	Clocked Override	clk-overid	1	
Timed Reminder	RC Aud Off	re-ringoff	1	
Timer	Timer	timer	1	
Trunk Identification [display button]	Trunk-ID	trk-id	1	
Trunk Group Name [display button]	Trunk-Name	trunk-name	1	
Visually Impaired Service (VIAS)	VIS	vis	1	
	Console Status	con-stat	1	
	Display	display	1	
	DTGS Status	dtgs-stat	1	
	Last Message	last-mess	1	
	Last Operation	last-op	1	
VDN of Origin Announcement Repeat	VOA Repeat	voa-repeat	1	12
VuStats	VuStats	vu-display	1	

1. List: List number 1 to 3 where the destination number is stored. DC: Dial codes of destination number.
2. Grp: The split group number for ACD.
3. Code: Enter a stroke code (0 through 9).
4. TAC: local-tgs — TAC of local TG

   remote-tgs — (L-TAC) TAC of TG to remote PBX

   remote-tgs — (R-TAC) TAC of TG on remote PBX

The combination of local-tgs/remote-tgs per console must not exceed 12 (maximum). Label associated button appropriately so as to easily identify the trunk group.

5. Grp: Enter a hundreds group number (1 through 20).
6. **Enhanced Hospitality** must be enabled on the System-Parameters Customer-Options (Optional Features) screen.
7. Ext: Can be a VDN extension.
8. Link: A link number — 1 to 8 for multi-carrier cabinets, 1 to 4 for single-carrier cabinets.
9. Grp: A trunk group number.
10. Grp: Group number of the hunt group.
11. Allows the attendant to alternate between active and split calls.
12. VDN of Origin must be enabled.

Setting Console Parameters

About this task

You can define system-wide console settings on the Console Parameters screen. For example, if you want to warn your attendants when there are more than 3 calls in queue or if a call waits for more than 20 seconds, complete the following steps:

Procedure

1. Type `change console-parameters`.
2. Press `Enter`
   The Console Parameters screen appears.
3. In the **Calls in Queue Warning** field, enter `3`.

   The system lights the console's second call waiting lamp if the number of calls waiting in the attendant queue exceeds 3 calls. Click **Next** to display page 2.
4. In the **Time in Queue Warning** field, enter `20`.

   The system issues a reminder tone if a call waits in the attendant queue for more than 20 seconds.
5. Press `Enter` to save changes.

   Note:

   Some of the settings on the individual Attendant Console screens can override your system-wide settings.

Removing an Attendant Console

About this task

Before you physically remove an attendant from your system, check the attendant's status, remove it from any group or usage lists, and then delete it from the system's memory. For example, to remove attendant 3, which also is assigned extension 4345:

Procedure

1. Type `status attendant 3`.
2. Press `Enter`.
   The Attendant Status screen appears.
3. Make sure that the attendant:
   - is plugged into the jack
   - is idle (not making or receiving calls)
4. Type `list usage extension 4345`.
5. Press `Enter`.
   The Usage screen shows where the extension is used in the system.
6. Press `Cancel`.
7. If the attendant extension appears on the Usage screen, access the appropriate feature screen and delete the extension.

   For example, if extension 1234 belongs to hunt group 2, type `change hunt group 2` and delete the extension from the list.
8. Type `remove attendant 3`.
9. Press `Enter`.
   The system displays the Attendant Console screen so you can verify that you are removing the correct attendant.
10. If this is the correct attendant, press `Enter`.

    If the system responds with an error message, the attendant is busy or still belongs to a group. Press **Cancel** to stop the request, correct the problem, and type `remove attendant 3` again.
11. Remove the extension from voice mail service if the extension has a voice mailbox.
12. Type `save translations`.
13. Press `Enter` to save your changes.

Note:

You do not need to delete the extension from coverage paths. The system automatically adjusts coverage paths to eliminate the extension.

Now you can unplug the console from the jack and store it for future use. You do not need to disconnect the wiring at the cross-connect field. The extension and port address remain available for assignment at a later date.

Providing Backup for an Attendant

Before you begin

- You can assign the attendant backup alerting only to multiappearance telephones that have a client room class of service (COS) set to No. For more information, see *Class of Service*.
- If you have not yet defined a Trunk Answer Any Station (TAAS) feature access code, you need to define one and provide the feature access code to each of the attendant backup users. For more information, see *Feature Access Code (FAC)*.

To enable your system to alert backup stations, you need to administer the Console Parameters screen for backup alerting. You also need to give the backup telephones an attendant queue calls feature button and train your backup users how to answer the attendant calls.

About this task

Communication Manager allows you to configure your system so that you have backup positions for your attendant. Attendant Backup Alerting notifies backup telephones that the attendant need assistance in handling calls. The backup telephones are alerted when the attendant queue reaches the queue warning level or when the console is in night service.

Once a backup telephone receives an alert, the user can dial the Trunk Answer Any Station (TAAS) feature access code (FAC) to answer the alerting attendant calls.

Tip:

You can find more information about attendant backup in the *GuestWorks Technician Handbook*.

Procedure

1. Type `change console-parameters`.
2. Press `Enter`.
   The Console Parameters screen appears.
3. In the **Backup Alerting** field, enter `y`.

4. Press `Enter` to save changes.

   The system will now notify anyone with an attendant queue calls button when the attendant queue reaches the warning level or when the console is in night service.

5. Type `change station 4345`.

6. Press `Enter`.
   The Station screen appears

7. In one of the Button Assignment fields, enter `atd-qcalls`.

   The atd-qcalls button provides the visual alerting for this telephone. When this button is dark (idle state), there are no calls in the attendant queue. When the button shows a steady light (busy state), there are calls in the attendant queue. When button shows a flashing light (warning state), the number of calls in the attendant queue exceeds the queue warning. The backup-telephone user also hears an alerting signal every 10 seconds.

8. Press `Enter` to save changes.

   Now you need to train the user how to interpret the backup alerting and give them the TAAS feature access code so that they can answer the attendant calls.

Chapter 9: Managing Telephone Displays

Display Administration

Displaying Caller Information

This chapter provides information on the messages that appear on the screens of display telephones.

Your system uses automatic incoming call display to provide information about incoming calls to a display telephone that is in use, or active on a call. The information is displayed for 30 seconds on all telephones except for CALLMASTER telephones, where the display goes blank after 30 seconds. However, the information for each new call overrides the existing message.

Call information appears on the display only if the call terminates at the telephone. For example, if the call is forwarded to another extension, no call information appears.

For more information on the buttons and languages you can set up for the messages that appear on the display, see the Telephone Displays feature description in the *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-505.

Displaying ANI Calling Party Information

About this task

Calling party information might consist of either a billing number that sometimes is referred to as Automatic Number Identification (ANI), or a calling party number. Your telephone might display the calling party number and name, or the incoming trunk group name.

To set up a tie trunk group to receive calling party information and display the calling party number on the telephone of the person called:

Procedure

1. Type `change trunk group nnnn`, where nnnn is the trunk group you want to change.
2. Click **Next Page** until you see the **Trunk Parameters** fields on the Trunk Group screen (page 2).
3. Type `tone` in the **Incoming Dial Type** field.

4. Click **Next Page** and type `*ANI*DNIS` in the **Incoming Tone (DTMF) ANI** field.
5. Press `Enter` to save your changes.

Displaying ICLID Information

Before you begin

Be sure the **Analog Trunk Incoming Call ID** field is set to y on the System-Parameters Customer-Options (Optional Features) screen. See the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207 for information on the required circuit pack.

About this task

Communication Manager collects the calling party name and number (Incoming Call Line Identification, or ICLID) received from the central office (CO) on analog trunks.

This example shows how to set up the analog diod trunk group 1 to receive calling party information and display the calling party number on the telephone of the person called.

Procedure

1. Type `change trunk group 1`.
   The Trunk Group screen for trunk group 1 appears. The **Group Type** field is already set to diod.
2. Click **Next Page** to display the **Trunk Features** fields on the Trunk Group screen (page 3).
3. Type `Bellcore` in the **Receive Analog Incoming Call ID** field.
4. Click **Next Page** to display the Administrable Timers screen.
5. Type `120` in the Incoming **Seizure (msec)** field.
6. Click **Enter** to save your changes.

Setting the Display Language

Procedure

1. Type `change station nnnn`, where nnnn is the extension of the station that you want to change.

2. Press **Enter**.
   The System displays the Station screen.
3. In the **Display Language** field, enter the display language you want to use.

   Tip:

   Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except english, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.).To display time in 24-hour format and display messages in English, set the **Display Language** field to `unicode`. When you enter unicode, the station displays time in 24-hour format, and if no Unicode file is installed, displays messages in English by default. For more information on Unicode, see *Administering Unicode display*.
4. Press **Enter** to save your changes.

Related topics:

Administering Unicode Display on page 221

Administering Unicode Display

To use Unicode display languages, you must have the appropriate Avaya Unicode Message files loaded on Communication Manager. These files are named avaya_unicode.txt (standard phone messages), custom_unicode.txt (posted messages and system labels), avaya_user-defined.txt (standard phone messages using Eurofont), and custom_user-defined.txt (posted messages and system labels using Eurofont).

To use the Phone Message files avaya_unicode.txt and custom_unicode.txt, you must have Unicode-capable stations, such as the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones, and Avaya Softphone R5.0. Unicode is also an option for the 2420J telephone when **Display Character Set** on the System Parameters Country-Options screen is katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide*, 555-250-701.

Only Unicode-capable stations have the script (font) support that is required to match the scripts that the Unicode Phone Message file uses. To use the user-defined messages files avaya_user-defined.txt and custom_user-defined.txt you must use an Avaya digital phone that supports Eurofont or Kanafont.

Note:

To view the dial pad letter/number/symbol mapping tables used for the integrated directory, see Telephone Display in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

For Communication Manager 2.2 and later, the following languages are available using Unicode display:

- Chinese
- Czech
- Danish
- Dutch
- German
- Hebrew
- Hungarian
- Icelandic
- Italian
- Japanese
- Korean
- Macedonian
- Polish
- Romanian
- Russian
- Servian
- Slovak
- Swedish
- Ukrainian

Obtaining and Installing Phone Message Files

About this task

A Unicode Message file for each supported language is available in a downloadable ZIP file on the Avaya support Web site (http://www.avaya.com/unicode). You can also create a new translation or edit an existing translation with the Avaya Message Editing Tool (AMET) (http://support.avaya.com/amet). Additional languages are periodically becoming available, so check this site often for the most up-to-date message files.

Note:

Refer to the *Communication Manager Messages Job Aid* for details on the following procedures.

Procedure

1. Download the appropriate Unicode message file to your PC. For an existing translation, download the desired language from http://www.avaya.com/unicode.
2. If necessary, create a new translation, or modify an existing translation, using the Avaya Message Editing Tool (AMET), available at http://support.avaya.com/amet.

Note:

Only the Avaya Message Editing Tool (AMET) can be used for translation edits, using any other editor will not update the Phone Message File correctly and such files will fail to install. See the *Avaya Message Editing Tool (AMET) Job Aid* in the Generic Phone Message Package file for more details on using AMET.

3. Transfer the Phone Message file to an Avaya S8XXX Server that is running Communication Manager 2.2 or later, using the Avaya Web pages, the Avaya Installation Wizard, or ftp.
4. Install Phone Message files with the Communication Manager System Management Interface (SMI). The Avaya Installation Wizard only supports install of Unicode Phone Message files. Note that the Installation Wizard is the same wizard that you use to transfer Phone Message files to an Avaya S8XXX Server that is running Communication Manager 2.2 or later.
5. The strings in a Communication Manager Phone Message File (avaya_unicode[2-4].txt, custom_unicode[2-4].txt, avaya_user-defined.txt, custom_user-defined.txt) are loaded in real-time into Communication Manager memory after you click the Install button on the “Communication Manager Phone Message File” page of Communication Manager SMI.
6. Set the **Display Language** field on the Station screen to `unicode`. Note that the keyword unicode only appears if a Unicode-capable telephone is entered in the Station screen **Type** field. To use a user-defined file, set the **Display Language** field on the Station screen to `user-defined`.

Note:

There is no uninstall option for Phone Message files. You can reload a new Phone Message file. This will overwrite existing Phone Message files.

Checking the Status of Phone Message File Loads

To verify that a Unicode Phone Message file is loaded correctly, run `status station xxxx` on any administered station. If the Unicode Phone Message file is loaded correctly, the **Display Messages Scripts** field on the second page contains the scripts that are in this file. The General Status screen for stations contains three Unicode script-related fields. To access the General Status screen, type `status station xxxx`, where xxxx is the extension of the station. The General Status screen appears. Click **Next** to display page 2 of the screen.

“Scripts” are a collection of symbols used to represent text in one or more writing systems. The three script fields shown in the UNICODE DISPLAY INFORMATION section are as follows:

- **Native Name Scripts**: Scripts supported in the Unicode station name.
- **Display Messages Scripts**: The scripts used in the Unicode Display Language.
- **Station Supported Scripts**: The scripts supported in the IP station that is registered to an extension.

Unicode Native Name support

Communication Manager supports Unicode for the “Name” associated with Vector Directory Numbers (VDNs), trunk groups, hunt groups, agent login id, vector names, station names, Invalid Number Dialed Display (Feature-Related System Parameters screen) and Restricted Number Dialed Display (Feature-Related System Parameters screen). The **Unicode Name** (also referred to as Native Name and Name 2) fields are hidden fields that are associated with the name fields you administer on the respective screens for each. These fields can only be administered using Avaya Site Administration (ASA)or MultiSite Administrator (MSA).

- The Unicode VDN name is associated with the name administered in the **Name** field on the Vector Directory screen. You must use MSA.
- The Unicode Trunk Group name is associated with the name administered in the **Group Name** field on the Trunk Group screen. You must use MSA.
- The Unicode Hunt Group Name is associated with the name administered in the **Group Name** field on the Hunt Group screen. You must use MSA.
- The Unicode Station Name is associated with the name administered in the **Name** field on the Station screen. You must use ASA or MSA.

Script Tags and Abbreviations

The following table defines the script tags and spells out the script abbreviations.

Script Numbe r	Script Tag Bit (hex)	Start Code.. End Code	Script or Block Name	SAT Screen Name
1	00000001	0000..007F	Basic Latin	Latn
2	00000002	0080..00FF	Latin-1 Supplement	Lat1
3	00000004	0100..017F	Latin Extended-A	LatA
4	00000008	0180..024F	Latin Extended-B	LatB
5	00000010	0370..03FF	Greek and Coptic	Grek
6	00000020	0400..04FF	Cyrillic	Cyrl

Script Numbe r	Script Tag Bit (hex)	Start Code.. End Code	Script or Block Name	SAT Screen Name
6	00000020	0500..052F	Cyrillic Supplementary	Cyrl
7	00000040	0530..058F	Armenian	Armn
8	00000080	0590..05FF	Hebrew	Hebr
9	00000100	0600..06FF	Arabic	Arab
10	00000200	0900..097F	Devanagari	Deva
11	00000400	0980..09FF	Bengali	Beng
12	00000800	0A00..0A7F	Gurmukhi	Guru
13	00001000	0A80..0AFF	Gujarati	Gujr
14	00002000	0B00..0B7F	Oriya	Orya
15	00004000	0B80..0BFF	Tamil	Taml
16	00008000	0C00..0C7F	Telugu	Telu
17	00010000	0C80..0CFF	Kannada	Knda
18	00020000	0D00..0D7F	Malayalam	Mlym
19	00040000	0D80..0DFF	Sinhala	Sinh
20	00080000	0E00..0E7F	Thai	Thai
21	00100000	0E80..0EFF	Lao	Laoo
22	00200000	1000..109F	Myanmar	Mymr
23	00400000	10A0..10FF	Georgian	Geor
32	80000000	1100..11FF	Hangul Jamo	Hang
24	00800000	1700..171F	Tagalog	Tglg
25	01000000	1780..17FF	Khmer	Khmr
27 28 29 30 31	04000000 08000000 10000000 20000000 40000000	2E80..2EFF	CJKV Radicals Supplement	Jpan ChiS ChiT Korn Viet
27 28 29 30 31	04000000 08000000 10000000 20000000 40000000	2F00..2FDF	Kangxi Radicals	Jpan ChiS ChiT Korn Viet
27 28 29	04000000 08000000 10000000	3000..303F	CJKV Symbols and Punctuation	Jpan ChiS ChiT

Script Numbe r	Script Tag Bit (hex)	Start Code.. End Code	Script or Block Name	SAT Screen Name
30 31	20000000 40000000			Korn Viet
27	04000000	3040..309F	Hiragana	Jpan
27	04000000	30A0..30FF	Katakana	Jpan
29	10000000	3100..312F	Bopomofo	ChiT
32	80000000	3130..318F	Hangul Compatibility Jamo	Hang
29	10000000	31A0..31BF	Bopomofo Extended	ChiT
27	04000000	31F0..31FF	Katakana Phonetic Extensions	Jpan
27 28 29 30 31	04000000 08000000 10000000 20000000 40000000	3200..32FF	Enclosed CJK Letters and Months	Jpan ChiS ChiT Korn Viet
27 28 29 30 31	04000000 08000000 10000000 20000000 40000000	3300..33FF	CJKV Compatibility	Jpan ChiS ChiT Korn Viet
27 28 29 30 31	04000000 08000000 10000000 20000000 40000000	3400..4DBF	CJKV Unified Ideographs Extension A	Jpan ChiS ChiT Korn Viet
27 28 29 30 31	04000000 08000000 10000000 20000000 40000000	4E00..9FFF	CJKV Unified Ideographs	Jpan ChiS ChiT Korn Viet
32	80000000	AC00..D7AF	Hangul Syllables	Hang
27 28 29 30 31	04000000 08000000 10000000 20000000 40000000	F900..FAFF	CJK Compatibility Ideographs	Jpan ChiS ChiT Korn Viet
	00000100	FB50..FDFF	Arabic Presentation Forms-A	Arab
27 28 29	04000000 08000000 10000000	FE30..FE4F	CJK Compatibility Forms	Jpan ChiS ChiT

Script Number	Script Tag Bit (hex)	Start Code.. End Code	Script or Block Name	SAT Screen Name
30 31	20000000 40000000			Korn Viet
	00000100	FE70..FEFF	Arabic Presentation Forms-B	Arab
26	02000000	FF00..FFEF	Halfwidth and Fullwidth Forms	Kana

Administering displays for QSIG trunks

About this task

Proper transmission of QSIG name data for display requires certain settings in the Trunk Group screen, the Signaling Group screen, and the System-Parameters Country-Options screen.

Procedure

1. Make the following changes to the Trunk Group screen.
   a. Set **Group Type** to `ISDN`
   b. Set **Character Set for QSIG Names** to `iso8859-1`
   c. Set **Outgoing Display** to `y`
   d. Set **Send Calling Number** to `y`
   e. Set **Send Name** to `y`
2. On the Signaling Group screen, set **Supplementary Service Protocol** to `b`.
3. On the System-Parameters Country-Options screen, set **Display Character Set** to `Roman`.

Fixing Problems

Symptom	Cause and Solution
Characters that display are not what you thought you entered.	This feature is case sensitive. Check the table to make sure that you entered the right case.
You entered `~c`, and `*` appears on the display instead.	Lower-case “c” has a specific meaning in Avaya Communication Manager, and therefore cannot be mapped to any other

Symptom	Cause and Solution
	character. An asterisk “*” appears in its place.
You entered ~−> or ~<− and nothing appears on the display.	These characters do not exist as single keys on the standard US-English keyboard. Therefore the system is not programmed to handle them.
Enhanced display characters appear in fields that you did not update.	If an existing display field contains a tilde (~) followed by Roman characters, and you update and submit that screen after this feature is activated, that field will display the enhanced character set.
Nothing displays on the terminal at all.	Some unsupported terminals do not display anything if a special character is presented. Check the model of display terminal that you are using.
You entered a character with a descender and part of it appears cut off in the display.	Some of the unused characters in Group2a have descenders that do not appear entirely within the display area. These characters are not included in the character map. For these characters (g,j,p,q,y), use Group1 equivalents.

Related Topics

See the Telephone Displays and the Administrable Display Languages feature descriptions in the *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205 for more information.

To view the dial pad letter/number/symbol mapping tables used for the integrated directory, see Telephone Display in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Setting the Directory Buttons

About this task

Your Communication Manager integrated directory contains the names and extensions that are assigned on each Station screen. Display-telephone users can use a telephone button to access the directory, use the touch-tone buttons to key in a name, and retrieve an extension from the directory.

Note:

When you assign a name beginning with two tildes (~~) to a telephone, and **Display Character Set** on the System Parameters Country-Options screen is set to Roman, the name does not appear in the integrated directory. Note that this is the only way to hide a name in the integrated directory.

The example below shows how to assign directory telephone buttons for extension 2000.

Our button assignment plan is set up so that telephone buttons 6, 7, and 8 are used for the directory. Remember, the name you type in the **Name** field on the first page of the Station screen is the name that appears when the integrated directory is accessed on a telephone display, except when the name is “hidden”, as described in the Note above.

Procedure

1. Type `change station 2000`.
2. Press `Enter`.
3. Press `Next Page` to move to the BUTTON ASSIGNMENTS section on Station screen (page 4).
4. In **Button Assignment** field 6, type `directory`.
5. In **Button Assignment** field 7, type `next`.
6. In **Button Assignment** field 8, type `call-display`.
7. Press `Enter` to save your changes.

Chapter 10: Handling Incoming Calls

Basic Call Coverage

What does call coverage do?

Basic incoming call coverage:

- Provides for automatic redirection of calls to alternate destinations when the called party is not available or not accepting calls
- Provides the order in which Communication Manager redirects calls to alternate telephones or terminals
- Establishes up to 6 alternate termination points for an incoming call
- Establishes redirection criteria that govern when a call redirects
- Redirects calls to a local telephone number (extension) or an off-switch telephone number (public network)

Redirection

Call coverage allows an incoming call to redirect from its original destination to an extension, hunt group, attendant group, uniform call distribution (UCD) group, direct department calling (DDC) group, automatic call distribution (ACD) split, coverage answer group, Audio Information Exchange (AUDIX), or vector for a station not accepting calls.

Adminstering system-wide call coverage characteristics

About this task

This section shows you how to set up system-wide call coverage characteristics that govern how coverage is handled.

The System Parameters Call Coverage/Call Forwarding screen sets up the global parameters which direct Communication Manager how to act in certain situations.

Procedure

1. Leave all default settings as they are set for your system.
2. If you desire to customize your system, carefully read and understand each field description before you make any changes.

For more information on redirecting calls, see *Covering calls redirected to an off-site location*.

For information on setting the Caller Response Interval before a call goes to coverage, see "Caller Response Interval" in the Call Coverage section of *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Creating coverage paths

About this task

This section explains how to administer various types of call coverage. In general, call coverage refers to what happens to incoming calls. You can administer paths to cover all incoming calls, or define paths for certain types of calls, such as calls to busy telephones. You can define where incoming calls go if they are not answered and in what order they reroute to other locations. For example, you can define coverage to ring the called telephone, then move to a receptionist if the call is not answered, and finally access a voice mailbox if the receptionist is not available.

With call coverage, the system redirects a call to alternate answering extensions when no one answers at the first extension. An extension can have up to 6 alternate answering points. The system checks each extension in sequence until the call connects. This sequence of alternate extensions is called a coverage path.

The system redirects calls based on certain criteria. For example, you can have a call redirect to coverage without ever ringing on the principal set, or after a certain number of rings, or when one or all call appearances (lines) are busy. You can set coverage differently for internal (inside) and external (outside) calls, and you can define coverage individually for different criteria. For example, you can decide that external calls to busy telephones can use the same coverage as internal calls to telephones with Do Not Disturb active.

Note:

If a call with a coverage path is redirected to a coverage point that is not available, the call proceeds to the next coverage point regardless of the type of coverage administered in the point that was unavailable. For example, if the unavailable coverage point has a hunt group coverage path administered, the hunt group coverage path would not be used by a call coming into the hunt group through the higher-level coverage path. The hunt group coverage path would be used only for calls coming directly into the hunt group extension.

Procedure

1. Type `add coverage path next`.
2. Press `Enter`.
   The system displays the Coverage Path screen. The system displays the next undefined coverage path in the sequence of coverage paths. Our example shows coverage path number 2.
3. Type a coverage path number in the **Next Path Number** field.

The next path is optional. It is the coverage path to which calls are redirected if the current path's coverage criteria does not match the call status. If the next path's criteria matches the call status, it is used to redirect the call; no other path is searched.

4. Fill in the **Coverage Criteria** fields.

   You can see that the default sets identical criteria for inside and outside calls. The system sets coverage to take place from a busy telephone, if there is no answer after a certain number of rings, or if the **DND** (do not disturb), **SAC** (send all calls), or **Go to Cover** button has been pressed or corresponding feature-access codes dialed.

5. Fill in the **Point** fields with the extensions, hunt group number, or coverage answer group number you want for coverage points.

   Each coverage point can be an extension, hunt group, coverage answer group, remote number, or attendant.

6. Click **Enter** to save your changes.

   Tip:

   If you want to see which extensions or groups use a specific coverage path, type `display coverage sender group n`, where `n` is the coverage path number. For example, you should determine which extensions use a coverage path before you make any changes to it.

Assigning a coverage path to users

About this task

Once you create a coverage path, assign it to a user. For example, we will assign the new coverage path to extension 2045.

Note:

A coverage path can be used for more than one extension.

Procedure

1. Type `change station 2054`.
2. Press `Enter`.
   The system displays the Station screen for extension 2054.
3. Type `2` in the **Coverage Path 1** field.

   To give extension 2054 another coverage path, you can type a coverage path number in the **Coverage Path 2** field.

4. Press `Enter` to save your changes.

Advanced call coverage

Advanced incoming call coverage:

- redirects calls based on time-of-day.
- allows coverage of calls that are redirected to sites not on the local server running Communication Manager.
- allows users to change back and forth between two coverage choices (either specific lead coverage paths or time-of-day tables).

Covering calls redirected to an off-site location

Before you begin

- On the System Parameters Customer-Options (Optional Features) screen, verify the **Coverage of Calls Redirected Off-Net Enabled** field is y. If not, contact your Avaya representative.
- You need call classifier ports for all situations except ISDN end-to-end signaling, in which case the ISDN protocol does the call classification. For all other cases, use one of the following:
    - Tone Clock with Call Classifier - Tone Detector circuit pack. See the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207 for more information on the circuit pack.
    - Call Classifier - Detector circuit pack.

About this task

You can provide coverage for calls that have been redirected to an off-site location (for example, your home). This capability, called Coverage of Calls Redirected Off-Net (CCRON) allows you to redirect calls onto the public network and bring back unanswered calls for further coverage processing.

Procedure

1. Type `change system-parameters coverage-forwarding`.
2. Press `Enter`.
3. Click **Next Page** until you see the **Coverage of Calls Redirected Off-Net (CCRON)** page of the System-Parameters Coverage-Forwarding screen.

4. In the **Coverage of Calls Redirected Off-Net Enabled** field, type `y`.
   This instructs Avaya Communication Manager to monitor the progress of an off-net coverage or off-net forwarded call and provide further coverage treatment for unanswered calls.
5. In the **Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point** field, leave the default as y.
6. In the **Ignore Network Answer Supervision** field, leave the default as n.
7. Click **Enter** to save your changes.

Defining coverage for calls redirected to external numbers

About this task

You can administer the system to allow calls in coverage to redirect to off-net (external) or public-network numbers.

You can use Standard remote coverage to an external number to send a call to an external telephone, but does not monitor the call once it leaves your system. Therefore, if the call is busy or unanswered at the external number, the call cannot be pulled back to the system. With standard remote call coverage, make the external number the last coverage point in a path.

Note:

Using remote coverage, you cannot cover calls to a remote voice mail.

With newer systems, you might have the option to use the Coverage of Calls Redirected Off-Net feature. If this feature is active and you use an external number in a coverage path, the system can monitor the call to determine whether the external number is busy or does not answer. If necessary, the system can redirect a call to coverage points that follow the external number. With this feature, you can have a call follow a coverage path that starts at the user's extension, redirects to the user's home telephone, and if not answered at home, returns to redirect to their voice mail box.

The call will not return to the system if the external number is the last point in the coverage path.

To use a remote telephone number as a coverage point, you need to define the number in the Remote Call Coverage Table and then use the remote code in the coverage path.

For example, to add an external number to coverage path 2:

Procedure

1. Type `change coverage remote`.
2. Press `Enter`.
   The system displays the Remote Call Coverage Table screen.

3. Type `93035381000` in one of the remote code fields.

   If you use a digit to get outside of your network, you need to add the digit before the external number. In this example, the system requires a ‘9’ to place outside calls.
4. Be sure to record the remote code number you use for the external number.

   In this example, the remote code is r01.
5. Click **Enter** to save your changes.
6. Type `change coverage path 2`.
7. Press `Enter`.
   The system displays the Coverage Path screen.

   Tip:

   Before making changes, you can use `display coverage sender group 2` to determine which extensions or groups use path 2.
8. Type `r1` in a coverage **Point** field.

   In this example, the coverage rings at extension 4101, then redirects to the external number. If you administer Coverage of Calls Redirected Off-Net and the external number is not answered or is busy, the call redirects to the next coverage point. In this example, the next point is Point 3 (h77 or hunt group 77).

   If you do not have the Coverage of Calls Redirected Off-Net feature, the system cannot monitor the call once it leaves the network. The call ends at the remote coverage point.
9. Click **Enter** to save your changes.

   Note:

   For more information on coverage, see "Call Coverage" in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Defining time-of-day coverage

About this task

The Time of Day Coverage Table on your system lets you redirect calls to coverage paths according to the time of day and day of the week when the call arrives. You need to define the coverage paths you want to use before you define the time of day coverage plan.

For example, let us say you want to administer the system so that incoming calls to extension 2054 redirect to a coworker in the office from 8:00 a.m. to 5:30 p.m., and to a home office from 5:30 p.m. to 8:00 p.m. on weekdays. You want to redirect the calls to voice mail after 8:00 p.m. weekdays and on weekends.

Procedure

1. Type `add coverage time-of-day next`.
2. Press `Enter`.
   The system displays the Time of Day Coverage Table screen, and selects the next undefined table number in the sequence of time-of-day table numbers. If this is the first time-of-day coverage plan in your system, the table number is 1.

   Record the table number so that you can assign it to extensions later.
3. To define your coverage plan, enter the time of day and path number for each day of the week and period of time.

   Enter time in a 24-hour format from the earliest to the latest. For this example, assume that coverage path 1 goes to the coworker, path 2 to the home, and path 3 to voice mail.

   Define your path for the full 24 hours (from 00:01 to 23:59) in a day. If you do not list a coverage path for a period of time, the system does not provide coverage for that time.
4. Click **Enter** to save your changes.
5. Now assign the time-of-day coverage to a user. For example, we use extension 2054:
   a. Type `change station nnnn`, where `nnnn` is the extension number.
   b. Press `Enter`.
   The system displays the Station screen.
   c. Move your cursors to Coverage Path 1 and type t plus the number of the Time of Day Coverage Table.
   d. Click **Enter** to save your changes.

   Now calls to extension 2054 redirect to coverage depending on the day and time that each call arrives.

Creating coverage answer groups

About this task

You can create a coverage answer group so that up to 8 telephones simultaneously ring when calls cover to the group. Anyone in the answer group can answer the incoming call.

Procedure

1. Enter `add coverage answer-group next`.
2. In the **Group Name** field, enter a name to identify the coverage group.

3. In the **Ext** field, type the extension of each group member.
4. Select **Enter** to save your new group list.

   The system automatically completes the Name field when you press Enter.

Call Forwarding

This section explains how to administer various types of automatic call forwarding. To provide call forwarding to your users, assign each extension a class of service (COS) that allows call forwarding. Then assign call-forwarding buttons to the user telephones (or give them the feature access code (FAC) for call forwarding) so that they can easily forward calls. Use the Station screen to assign the COS and any call-forwarding buttons.

Within each class of service, you can determine whether the users in that COS have the following call forwarding features:

- Call Forwarding All Calls — allows users to redirect all incoming calls to an extension, attendant, or external telephone number.
- Call Forwarding Busy/Don't Answer — allows users to redirect calls only if their extensions are busy or they do not answer.
- Restrict Call Fwd-Off Net — prevents users from forwarding calls to numbers that are outside your system network.

As the administrator, you can administer system-wide call-forwarding parameters to control when calls are forwarded. Use the System Parameters Call Coverage/Call Forwarding screen to set the number of times an extension rings before the system redirects the call because the user did not answer (CFWD No Answer Interval). For example, if you want calls to ring 4 times at an extension and, if the call is not answered, redirect to the forwarding number, set this parameter to 4.

You also can use the System Parameters Call Coverage/Call Forwarding screen to determine whether the forwarded-to telephone can override call forwarding to allow calls to the forwarded-from telephone (Call Forward Override). For example, if an executive forwards incoming calls to an attendant and the attendant needs to call the executive, the call can be made only if the **Call Forwarding Override** field is set to y.

Determining extensions having call forwarding activated

Procedure

1. Type `list call-forwarding`.
2. Press `Enter`.

This command lists all the extensions that are forwarded along with each forwarding number.

Note:

If you have a V1, V2, or V3 system, you can see if a specific extension is forwarded only by typing `status station nnnn`, where `nnnn` is the specific extension.

For more information see “Call Forwarding” in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Setting up call forwarding for users

About this task

This section shows you how to give your users access to call forwarding.

We will change a call forwarding access code from a local telephone with a Class of Service of 1:

Procedure

1. Type `change feature-access-codes`.
2. Press `Enter`.
   The system displays the Feature Access Code (FAC) screen.
3. In the **Call Forwarding Activation Busy/DA** field, type `*70`.
   The *70 feature access code activates the call forwarding option so incoming calls forward when your telephone is busy or does not answer.
4. In the **Call Forwarding Activation All** field, type `*71`.
   The *71 feature access code forwards all calls.
5. In the **Call Forwarding Deactivation** field, type `#72`.
   The #72 feature access code deactivates the call forwarding option.
6. Press `Enter` to save your changes.
7. Type `change cos`.
8. Press `Enter`.
   The system displays the Class of Service screen.
9. On the **Call Fwd-All Calls** line, in the 1 column, type `y`.
   This allows the user with this Class of Service to forward their calls. The 1 column is for telephones with a Class of Service of 1.
10. On the **Console Permissions** line, in the 1 column, type `y`.

This allows the user to define call forwarding on any station, not just the dialing station.

11. On the **Restrict Call Fwd-Off Net** line, in the 1 column, type `y`.
    This restricts your users from forwarding calls off-site. If you want your users to be able to call off-site, leave this field as n.
12. On the **Call Forward Busy/DA** line, in the 1 column, type `y`.
    This forwards a user's calls when the telephone is busy or doesn't answer after a programmed number of rings.
13. Press `Enter` to save your changes.

Allowing users to specify a forwarding destination

About this task

Now that you have set up system-wide call forwarding, have your users use this procedure if they want to change their call forwarding destination from their work (local) station.

Procedure

1. They dial either their Call Forwarding Activation Busy/DA or Call Forwarding Activation All feature access code. If your users have buttons assigned, they press those buttons, listen for dial tone, and dial the digits.

   Note:

   Both Call Forwarding Activation Busy/DA or the Call Forwarding Activation All cannot be active for the same telephone at the same time.

   In this example, enter `*71` for Call Forwarding Activation All.
2. They dial their "forwarding-to" off-site or on-site number.

   In this example, enter `2081`. This is a local number; for off-site forwarding, include the AAR/ ARS feature access code.
3. When they hear the 3-beep confirmation tone, they hang up.

Changing the forwarding destination remotely

About this task

Now that you have set up all of the required system administration for call forwarding, have your users use this procedure if they want to change their call forwarding destination from a telecommuting (off-site) telephone.

Procedure

1. They dial their telecommuting extension.

   In this example, enter `555-9126`.
2. When they get dial tone, they dial either their Extended Call Forward Activate Busy/ DA or the Extended Call Forward Activate All feature access code.

   In this example, enter `*61` for the Extended Call Forward Activate All number.
3. When they get dial tone, they dial their extension number. Press the `#`.

   In this example, enter `1014`, then `#`.
4. Even though there is no dial tone, they dial their security code. Press `#`.

   In this example, enter `4196`, then `#`.
5. When they get dial tone, they dial their "forwarding-to" off-site or on-site number.

   In this example, enter `9-555-2081`.
6. When they hear the 3-beep confirmation tone, they hang up.

Allowing users to change coverage remotely

About this task

This section shows you how to allow users to change their call coverage path from a local or telecommuting (off-site) telephone.

Procedure

1. Type `change feature-access-codes`.
2. Press `Enter`.
   The system displays the Feature Access Code (FAC) screen.
3. In the **Change Coverage Access Code** field, type `*85`.

   Use the *85 feature access code to change a coverage path from a telephone or remote station.
4. Press `Enter` to save your changes.
5. Type `change cor`.
6. Press `Enter`.
   The system displays the Class of Restriction screen.
7. In the **Can Change Coverage** field, type `y`.

   This permits users to select one of two previously administered coverage paths.
8. Press `Enter` to save your changes.

9. Type `change station 1014`.
10. Press `Enter`.
    The system displays the Station screen for extension 1014.
11. In the **Security Code** field, type `4196`.

    In this example, this is your security code.
12. In the **Coverage Path 1** and **Coverage Path 2** fields, verify that both are defined enabling your user to move from one coverage path to another.

    The t1 and t2 are the numbers of the Time of Day Coverage Tables.
13. Press `Enter` to save your changes.

Enhanced Call Forwarding

There are three types of Enhanced Call Forwarding:

- Use Enhanced Call Forwarding Unconditional to forward all calls
- Use Enhanced Call Forwarding Busy to forward calls when the user's line is busy
- Use Enhanced Call Forwarding No Reply to forward calls when the user does not answer the call

The user can activate or deactivate any of these three types from their phone, and can specify different destinations for calls that are from internal and external sources. Users receive visual display and audio feedback on whether or not Enhanced Call Forwarding is active.

Display messages on the phone guide the user through the process of activating and de-activating Enhanced Call Forwarding, and for viewing the status of their forwarding.

Users can choose whether they want, at any one time, Call Forwarding or Enhanced Call Forwarding activated. The regular Call Forwarding feature (called "Classic Call Forwarding" to distinguish it from Enhanced Call Forwarding) continues to be available to users and has not changed.

Each of the three types of Enhanced Call Forwarding can have different destinations based on whether a call is internal or external. Therefore, six different destinations are possible to set up:

- Enhanced Call Forwarding Unconditional - internal
- Enhanced Call Forwarding Unconditional - external
- Enhanced Call Forwarding Busy - internal
- Enhanced Call Forwarding Busy - external
- Enhanced Call Forwarding No Reply - internal
- Enhanced Call Forwarding No Reply - external.

Each of these types of call forwarding can be activated either by feature access codes or by feature button.

When Enhanced Call Forwarding is deactivated, the destination number is kept. When the user activates Enhanced Call Forwarding again, the same destination number can be used without having to type it again.

When Enhanced Call Forwarding is not activated for a call, the call will go to a coverage path, if one has been set up.

Redirection

Call coverage allows an incoming call to redirect from its original destination to an extension, hunt group, attendant group, uniform call distribution (UCD) group, direct department calling (DDC) group, automatic call distribution (ACD) split, coverage answer group, Audio Information Exchange (AUDIX), or vector for a station not accepting calls.

Activating Enhanced Call Forwarding Using a feature button

Procedure

1. Press the feature button labeled cfwd-enh
   The phone goes off hook.
2. Press `1` to activate Enhanced Call Forwarding.
3. Press
   - `1` for Enhanced Call Forwarding Unconditional
   - `2` for Enhanced Call Forwarding Busy
   - `3` for Enhanced Call Forwarding No Reply
4. Press
   - `1` to forward internal calls
   - `2` to forward external calls
   - `3` to forward all calls
5. Dial the destination number to which calls will be forwarded.

   Dial `#` at the end of an external destination number, or wait for the timeout to expire.

   You hear a confirmation tone if the activation was successful.

Activating Enhanced Call Forwarding Using a feature access code

Procedure

1. Press the feature access code for activating Enhanced Call Forwarding.
   The phone goes off hook.
2. Press
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 for Enhanced Call Forwarding No Reply
3. Press
   - 1 to forward internal calls
   - 2 to forward external calls
   - 3 to forward all calls
4. Dial the destination number to which calls will be forwarded.

   Dial # at the end of an external destination number, or wait for the timeout to expire.

   You hear a confirmation tone if the activation was successful.

Deactivating enhanced call forwarding using a feature button

Procedure

1. Press the feature button labeled **cfwd-enh**.
   The phone goes off hook.
2. Press `2` to deactivate Enhanced Call Forwarding.
3. Press
   - `0` for all Enhanced Call Forwarding
   - `1` for Enhanced Call Forwarding Unconditional
   - `2` for Enhanced Call Forwarding Busy
   - `3` for Enhanced Call Forwarding No Reply
4. Press
   - `1` for internal calls

- 2 for external calls
- 3 for all calls

You hear a confirmation tone if the deactivation was successful.

Deactivating enhanced call forwarding using a feature access code

Procedure

1. Press the feature access code for deactivating Enhanced Call Forwarding.
   The phone goes off hook.
2. Press
   - 0 to deactivate all Enhanced Call Forwarding
   - 1 to deactivate Enhanced Call Forwarding Unconditional
   - 2 to deactivate Enhanced Call Forwarding Busy
   - 3 to deactivate Enhanced Call Forwarding No Reply
3. Press
   - 1 for internal calls
   - 2 for external calls
   - 3 for all calls

   You hear a confirmation tone if the deactivation was successful.

Reactivating enhanced call forwarding using a feature button

Procedure

1. Press the feature button labeled **cfwd-enh**.
   The phone goes off hook.
2. Press 1to reactivate Enhanced Call Forwarding
3. Press
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 for Enhanced Call Forwarding No Reply

4. Press
    - 1 to forward internal calls
    - 2 to forward external calls
    - 3 to forward all calls
5. Optionally, dial the destination number to which calls will be forwarded.

    If you do not enter a destination number, the previous destination number will be used.

    Dial # at the end of an external destination number, or wait for the timeout to expire.

    You hear a confirmation tone if the action was successful.

Reactivating enhanced call forwarding using a feature access code

Procedure

1. Press the feature access code for activating Enhanced Call Forwarding.
    The phone goes off hook.
2. Press
    - 1 for Enhanced Call Forwarding Unconditional
    - 2 for Enhanced Call Forwarding Busy
3. Press
    - 1 to forward internal calls
    - 2 to forward external calls
    - 3 to forward all calls
4. Optionally, dial the destination number to which calls will be forwarded.

    If you do not enter a destination number, the previous destination number will be used.

    Dial # at the end of an external destination number, or wait for the timeout to expire.

    You hear a confirmation tone if the action was successful.

Displaying Enhanced Call Forwarding Status Using a Feature Button

Procedure

1. Press the feature button labeled **cfwd-enh**.
   The phone goes off hook.
2. Press `3` to display status.
   Your phone will display the status of the different types of Enhanced Call Forwarding.

Displaying Enhanced Call Forwarding Status Using a Feature Access Code

Procedure

1. Press the feature access code for displaying Enhanced Call Forwarding status..
   The phone goes off hook.
2. Press 3 to display status.
   Your phone will display the status of the different types of Enhanced Call Forwarding.

Activating Enhanced Call Forwarding from an off-network phone

Procedure

1. Dial the remote access number, including barrier code or authentication code.
2. Press the feature access code for activating Enhanced Call Forwarding.
3. Press:
   - `1` for Enhanced Call Forwarding Unconditional
   - `2` for Enhanced Call Forwarding Busy
   - `3` for Enhanced Call Forwarding No Reply
4. Press
   - `1` to forward internal calls

- 2 to forward external calls
- 3 to forward all calls

5. Dial the forwarding station extension.
6. Dial the destination number to which calls will be forwarded.

   Dial # at the end of an external destination number, or wait for the timeout to expire.

   You hear a confirmation tone if the activation was successful.

Deactivating Enhanced Call Forwarding from an off-network phone

Procedure

1. Dial the remote access number, including barrier code or authentication code.
2. Press the feature access code for deactivating Enhanced Call Forwarding.
3. Press:
   - 0 for all Enhanced Call Forwarding
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 for Enhanced Call Forwarding No Reply
4. Press
   - 1 for internal calls
   - 2 for external calls
   - 3 for all calls
5. Dial the forwarding station extension.
6. Dial the destination number to which calls will be forwarded.

   You hear a confirmation tone if the activation was successful.

Activating Enhanced Call Forwarding from a phone with console permissions

Procedure

1. Press the feature access code for activating Enhanced Call Forwarding.
   The phone goes off hook.
2. Press:
   - `1` to forward internal calls
   - `2` to forward external calls
   - `3` to forward all calls
3. Dial the forwarding station extension.
4. Dial the destination number to which calls will be forwarded.

   Dial `#` at the end of an external destination number, or wait for the timeout to expire.

   You hear a confirmation tone if the activation was successful.

Deactivating Enhanced Call Forwarding from a phone with console permission

Procedure

1. Press the feature access code for activating Enhanced Call Forwarding.
   The phone goes off hook.
2. Press:
   - `0` for all Enhanced Call Forwarding
   - `1` for Enhanced Call Forwarding Unconditional
   - `2` for Enhanced Call Forwarding Busy

Night Service

You can use night service to direct calls to an alternate location when the primary answering group is not available. For example, you can administer night service so that anyone in your marketing department can answer incoming calls when the attendant is at lunch or has left for the day.

Once you administer night service to route calls, your end-users merely press a button on the console or a feature button on their telephones to toggle between normal coverage and night service.

There are five types of night service:

- Night Console Night Service — directs all attendant calls to a night or day/night console
- Night Station Night Service — directs all incoming trunk or attendant calls to a night service destination
- Trunk Answer from Any Station (TAAS) — directs incoming attendant calls and signals a bell or buzzer to alert other employees that they can answer the calls
- Trunk Group Night Service — directs incoming calls to individual trunk groups to a night service destination
- Hunt Group Night Service — directs hunt group calls to a night service destination

Setting up night station service to voice mail

About this task

The night station service (also known as Listed Directory Number (LDN) Night Service) sends calls directed to an LDN to voice mail when the system is in night service.

What is described below is a common setup; however, you can use a regular extension in this field, but it will not follow coverage.

Note:

You can use a dummy hunt group (one with no members) or an exported station with a coverage path. The instructions below use a hunt group.

Procedure

1. Type `add hunt-group next`.
2. Press `Enter`.
   The system displays the Hunt Group screen.

   The **Group Number** field fills automatically with the next hunt group number.
3. In the **Group Name** field, type the name of the group.

   In our example, type `ldn nights`. There should be no members in this hunt group.
4. Click **Enter** to save your changes.

Note:

If you are using tenant partitioning, the command for the next step will be `change tenant x`. If you are using tenant partitioning, the **Night Destination** field does not appear on the Listed Directory Numbers screen. Instead, it is on the Tenant screen.

5. Type `change listed-directory-numbers`.
6. Press `Enter`.
   The system displays the Listed Directory Numbers screen.
7. In the **Night Destination** field, add the night destination on the listed directory telephone.

   In our example, type `51002`.
8. Click **Enter** to save your changes.
9. Type `change console-parameters`.
10. Press `Enter`.
    The system displays the Console Parameters screen.
11. In the **DID-LDN Only to LDN Night Ext** field, type `n`.
12. Click **Enter** to save your changes.
13. From a telephone with console permissions, dial the call forwarding feature access code, then the hunt group's extension, followed by the main number of AUDIX.

    In our example, dial 51002.

    Note:

    You should receive the confirmation tone (3 beeps). This step is very important as calls to the LDN night service extension do not follow coverage.
14. In voice mail, build your auto attendant with the extension of the Listed Directory Number, not the hunt group.

    The originally dialed number was the LDN. That is what Communication Manager passes to the voice mail. In the case of the INTUITY and newer embedded AUDIX Voice Mail systems, you can use the Auto Attendant routing table to send the calls to a common Auto Attendant mailbox.

Setting up night console service

About this task

Night Console Service directs all calls for primary and daytime attendant consoles to a night console. When a user activates Night Console Service, the Night Service button for each attendant lights and all attendant-seeking calls (and calls waiting) in the queue are directed to the night console.

Note:

Activating night console service also puts trunk groups into night service, except those for which a night service button has been administered. See Setting up trunk answer from any stationSetting up trunk answer from any station on page 244 for more information.

To activate and deactivate Night Console Service, the attendant typically presses the Night button on the principal attendant console or designated console.

Only the principal console can activate night service. In the absence of any console, a telephone can activate night service.

We will put the attendant console (attendant 2) in a night service mode.

Procedure

1. Type `change attendant`.
2. Press `Enter`.
   The system displays the Attendant Console screen.
3. In the **Console Type** field, type `principal`.

   There can be only one night-only or one day/night console in the system unless you administer Tenant Partitioning. Night Service is activated from the principal console or from the one station set per-system that has a **nite-serv** button.
4. Click **Enter** to save your changes.

Setting up night station service

About this task

You can use night station service if you want to direct incoming trunks calls, DID-LDN (direct inward dialing-listed directory number) calls, or internal calls to the attendant (dialed 'O' calls) to a night service destination.

Let us say your attendant, who answers extension (LDN) 8100, usually goes home at 6:00 p.m. When customers call extension 8100 after hours, you would like them to hear an announcement that asks them to try their call again in the morning.

To set up night station service, you need to record the announcement (in our example, it is recorded at announcement extension 1234).

Tip:

All trunk groups that are routed through the attendant direct to this night service destination provided they already do not have a night service destination and, on the Console

Parameters screen, the **DID-LDN Only to DID-LDN Night Ext** field is n. See *Setting up trunk answer from any station*.

Procedure

1. Type `change listed-directory-numbers`.
2. Press `Enter`.
   The system displays the Listed Directory Numbers screen.
3. Enter `1234` in the **Night Destination** field.

   The destination can be an extension, a recorded announcement extension, a vector directory number, or a hunt group extension.
4. Click **Enter** to save your changes.
5. Type change console-parameters.
6. Press Enter.
   The system displays the Console Parameters screen.
7. In the **DID-LDN Only to LDN Night Extension** field, type `n`.
8. Click Enter to save your changes.

   After you set up night station service, have the attendant use the night console button to activate and deactivate night service.

Setting up trunk answer from any station

About this task

There might be situations where you want everyone to be able to answer calls when the attendant is away. Use trunk answer any station (TAAS) to configure the system so that it notifies everyone when calls are ringing. Then, you can give users the trunk answer any station feature access code so they can answer these calls.

When the system is in night service mode, attendant calls redirect to an alerting device such as a bell or a buzzer. This lets other people in the office know when they should answer the telephone.

Note:

If no one answers the call, the call will not redirect to night service.

We will define a feature access code (we'll use 71) and configure the alerting device for trunk answer any station.

You need a ringing device and 1 port on an analog line circuit pack. See the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207, for more information on the circuit pack.

Procedure

1. Type `change feature-access-codes`.
2. Press `Enter`,
   The system displays the Feature Access Code (FAC) screen.
3. Click **Next** until you see the T**runk Answer Any Station Access Code** field.
4. In the **Trunk Answer Any Station Access Code** field, type `71`.
5. Click **Enter** to save your changes.

   Once you set the feature access code, determine where the external alerting device is connected to the Communication Manager server (we'll use port 01A0702).

   To set up external alerting:
6. Type `change console-parameters`.
7. Press `Enter`.
   The system displays the Console Parameters screen.
8. In the **EXT Alert Port (TAAS)** field, type `01A0702`.

   Use the port address assigned to the external alerting device.
9. In the **EXT Alert Port (TAAS)** field, type `01A0702`.
10. Click **Enter** to save your changes.

Setting up external alerting

Procedure

1. Type `change console-parameters`.
2. Press `Enter`.
   The system displays the Console Parameters screen.
3. In the **EXT Alert Port (TAAS)** field, type `01A0702`.

   Use the port address assigned to the external alerting device.
4. Click **Enter** to save your changes.

Setting up external alerting night service

About this task

Calls redirected to the attendant via Call Forwarding or Call Coverage will not go to the LDN Night Station. If there is no night station specified, and the TAAS bell is being used, these calls ring the TAAS bell. A call following the coverage path rings the TAAS bell for the number of times indicated in the Coverage Don't Answer Interval for Subsequent Redirection (Rings) field. If not answered, the call proceeds to the next point in the station's coverage path. If the call was sent to the Attendant by Call Forwarding, it continues to ring the TAAS bell.

When night service is enabled, and there is a night service destination on the Listed Directory Numbers screen, calls covering to the attendant attempt to ring the night destination instead of the attendant position even if the handset is plugged in.

To send LDN calls to the attendant during the day and to a guard's desk at night:

Procedure

1. Type `change listed-directory-numbers`.
2. Press `Enter`.
   The system displays the Listed Directory Numbers screen.
3. In the **Night Destination** field, verify this field is blank.
4. Click **Enter** to save your changes.
5. Type `change console-parameters`.
6. Press `Enter`.
   The system displays the Console Parameters screen.
7. In the `EXT Alert Port (TAAS)` field, type `01A0702`.

   This is the port address assigned to the external alerting device.
8. Click **Enter** to save your changes.

   The system is in Night Service.

   Any calls to extension 2000 now go to extension 3000 (the guard's desk).

   Any "0" seeking calls go to extension 3000 (the guard's desk).

Sending LDN calls to the attendant during the day and to the TAAS bell at night

Procedure

1. Type `change console-parameters`.
2. Press `Enter`.
   The system displays the Console Parameters screen.
3. In the **DID-LDN Only to Night Ext?**field, type `y`.
   This allows only listed directory number calls (LDN) to go to the listed directory night service number extension.

4. In the **Ext Alert Port (TAAS)** field, type `01A070`.

   This is the port address assigned to the external alerting device.

5. Click **Enter** to save your changes.

   Any DNIS extension 2000 calls now go to the TAAS bell.

   Any “0” seeking calls now go to the TAAS bell.

Setting up trunk group night service

About this task

You can use trunk group night service if you want to direct individual trunk groups to night service. The system redirects calls from the trunk group to the group’s night service destination.

Trunk group night service overrides night station service. For example, we will say you activate trunk group night service, and then your attendant activates night station service. In this case, calls to the trunk group use the trunk night service destination, rather than the station night service destination.

We will direct night calls for trunk group 2 to extension 1245.

Procedure

1. Type `change trunk-group`.
2. Press `Enter`.

   The system displays the Trunk Group screen.
3. Type `1245` in the **Night Service** field.

   The destination can be a station extension, a recorded announcement extension, a vector directory number, a hunt group extension, a terminating extension group, or attd if you want to direct the call to the attendant.
4. Click **Enter** to save your changes.

Setting up night service for hunt groups

About this task

You can administer hunt group night service if you want to direct hunt group calls to a night service destination.

Let us say your helpline on hunt group 3 does not answer calls after 6:00 p.m. When customers call after hours, you would like them to hear an announcement that asks them to try their call again in the morning.

To set up night service for your helpline, you need to record the announcement (in our example, the announcement is on extension 1234) and then modify the hunt group to send calls to this extension.

Procedure

1. Type `change hunt-group`.
2. Press `Enter`.
   The system displays the Hunt Group screen for hunt group 3.
3. In the **Night Service Destination** field, type `1234`.

   The destination can be an extension, a recorded announcement extension, a vector directory number, a hunt group extension, or attd if you want to direct calls to the attendant.

   Calls to hunt group 3 will follow the coverage path assigned to extension 1234.
4. Click **Enter** to save your changes.
5. Now you need to program a night service button.

Related topics:

Hunt Groups on page 278

Call Pickup

Users might need to answer a call that is ringing at a nearby desk. With Communication Manager, a user can answer a call that is ringing at another telephone in three ways:

- Use Call Pickup. With Call Pickup, you create one or more pickup groups. A pickup group is a collection, or list, of individual telephone extensions. A pickup group is the way to connect individual extensions together. For example, if you want everyone in the payroll department to be able to answer calls to any other payroll extension, you can create a pickup group that contains all of the payroll extensions.

  A user extension can belong to only one pickup group. Also, the maximum number of pickup groups might be limited by your system configuration.

  Using their own telephones, all members in a pickup group can answer a call that is ringing at another group member telephone. If more than one telephone is ringing, the system selects the extension that has been ringing the longest.
- Use Extended Call Pickup. With Extended Call Pickup, you can define one or more extended pickup groups. An extended pickup group is the way to connect individual pickup groups together.

There are two types of extended pickup groups: simple and flexible. You administer the type of extended pickup groups on a system-wide basis. You cannot have both simple and flexible extended pickup groups on your system at the same time.

Based on the type of extended pickup group that you administer, members in one pickup group can answer calls to another pickup group.

For more information, see *Setting up simple extended pickup groups*, *Setting up flexible extended pickup groups*, and *Changing extended pickup groups*.

- Use Directed Call Pickup. With Directed Call Pickup, users specify what ringing telephone they want to answer. A pickup group is not required with Directed Call Pickup. You must first administer Directed Call Pickup before anyone can use this feature.

For more information, see *Setting up Directed Call Pickup*.

Throughout this procedure on pickup groups and extended pickup groups, we show examples to make Call Pickup easier to understand.

Call Pickup Alert

Members of a call pickup group know that another group member is receiving a call in two ways:

- Group members can hear the other telephone ring.
- The Call Pickup button status lamp on the telephones of all the group members flash.

Note:

You must activate Call Pickup Alerting in your system, and assign a Call Pickup button to the telephones of each pickup group member, before the Call Pickup button status lamps work properly.

For information how to set up Call Pickup Alerting, see Enabling Call Pickup Alerting.

If the **Call Pickup Alerting** field on the Feature-Related System Parameters screen is set to n , members of the call pickup group must rely only on ringing to know when another group member receives a call. Pickup group members must be located close enough that they can hear the ringing of the other telephones.

To answer a call, a pickup group member can either press the Call Pickup button on the telephone, or dial the Call Pickup feature access code (FAC).

For more information, see Assigning a Call Pickup button to a user telephone, and Assigning a Call Pickup feature access code.

The Call Pickup Alerting feature is enhanced to support the SIP telephones. You need to upgrade the SIP telephone firmware 2.6 to take advantage of call pickup alerting on SIP telephones. You can activate an audible and a visual alert at a SIP telephone by administering the **Call Pickup Ring Type** and **Call Pickup Indication** fields available under the Screen and Sound Options menu on the SIP telephones.

For more information on how to administer the audible and visual alerting, see the user guide for your SIP telephone.

The **Call Pickup Alerting** field on the Feature-Related System Parameters screen determines how the Call Pickup button status lamps operate.

- If the **Call Pickup Alerting** field is set to n, the Call Pickup Button status lamps on all pickup group member telephones do not flash when a call comes in. When a pickup group member hears the telephone of another group member ring and presses the Call Pickup button to answer the call, the:
    - Call Pickup button status lamp of the answering group member becomes steadily lit for the duration of the call.
    - Telephone of the called group member stops ringing.
- If the **Call Pickup Alerting** field is set to y, the Call Pickup Button status lamps on all pickup group member telephones flash when a call comes in. When a pickup group member sees the Call Pickup button status lamp flash and presses the Call Pickup button to answer the call, the:
    - Call Pickup button status lamp of the answering group member goes out.
    - Call Pickup button status lamp of the called group member goes out.
    - Call Pickup button status lamps of the other pickup group members go out.
    - Telephone of the called group member stops ringing.

If another call comes into the pickup group,

- The call will alert to the answering group member. However, the answering group member cannot answer the call using the call pickup button unless the member puts the original call on hold. Once the group member is off the original call, that member is alerted for subsequent group calls and can answer the call using the call pickup button.
- The call alerts to all other group members and can be answered by any of these other group members.

In all scenarios, the call appearance button on the telephone of the called group member:

- Stays steadily lit if the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to y. The called group member can join the call in progress by pressing the lit call appearance button. The person who picked up the call can either stay on the call or hang up.
- Goes out if the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to n. The called group member cannot join the call in progress.

The system uses an algorithm to select what call is answered when multiple calls ring or alert in a call pickup group at the same time. The system searches the extensions of the call pickup group until the system finds an extension with a call that is eligible to be answered with Call

Pickup. The system selects this call to be answered. The next time that a group member answers a call with Call Pickup, the system bypasses the extension that was answered most recently, and starts the search at the next extension.

For example, if a group member attempts to use Call Pickup when two calls are ringing at extension A and one call is ringing at extension B, the system selects the calls in the following order:

- One of the calls to extension A
- The call to extension B
- The remaining call to extension A

The system also determines which call that a group member answers when multiple calls ring or alert at the same telephone. The system selects the call with the lowest call appearance, which is usually the call appearance that is nearest to the top of the telephone.

For example, when calls ring or alert at the second and the third call appearances, the system selects the call on the second call appearance for the user to answer.

Setting up Call Pickup

About this task

The first step in setting up any call pickup system is to create pickup groups and assign users to the groups. You can create one or many pickup groups, depending on your needs. A user extension can belong to only one pickup group.

In this exercise, you will:

- Add a pickup group and assign users to the pickup group.
- Enable Call Pickup alerting.
- Assign a Call Pickup button to each extension in the pickup group.
- Assign a feature access code (FAC).

Adding Pickup Groups

Procedure

1. Type `add pickup-group next`.
2. Press `Enter`.
   The system displays the Pickup Group screen. The system also assigns the next available Group Number for the new pickup group.

   Note:

   The **Extended Group Number** field is not shown in this example because the system is set for none or simple extended pickup groups. For more information, see *Setting up simple extended pickup groups*. If the **Extended Group Number** field is visible on this screen, then your system is set up for flexible extended pickup groups.

For more information, see *Setting up flexible extended pickup groups*.

3. Type a name for this pickup group in the **Group Name** field.
4. Type the extension of each group member.
   Up to 50 extensions can belong to one pickup group.
5. Click **Enter** to save your changes.
   The system automatically completes the **Name** field when you click **Enter**.

Example

This procedure shows how to set up a new pickup group 11 for Accounting. For the rest of these procedures, let us say that you also set up these pickup groups:

- 12 for Billing
- 13 for Credit Services
- 14 for Delinquency Payments
- 15 for Executives
- 16 for Finance

Related topics:

Simple extended pickup groups on page 267

Flexible Extended Pickup Groups on page 270

Enabling Call Pickup Alerting

About this task

Call Pickup Alerting allows members of pickup groups to know visually when the telephone of another member is ringing. Use Call Pickup Alerting if the telephones of other pickup group members are too far away to be heard. You must enable Call Pickup Alerting in your system.

Procedure

1. Enter `change system-parameters features`.
2. Click **Next** until you see the **Call Pickup Alerting** field.
3. Set the **Call Pickup Alerting** field to `y`.
4. Select **Enter** to save your changes.

Related topics:

Call Pickup Alert on page 258

Assigning a Call Pickup button to a user telephone

About this task

After you define one or more pickup groups, assign a Call Pickup button for each extension in each pickup group. Users in a pickup group can press the assigned Call Pickup button to answer calls to any other extension in their pickup group.

Procedure

1. Type `change station` *`n`*, where *n* is an extension in the pickup group.
2. Press `Enter`.
   The system displays the Station screen.
3. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
4. Type `call-pkup` after the button number.
5. Press **Enter** to save your changes.

   Repeat this procedure for each member of each pickup group.

Assigning a Call Pickup feature access code

About this task

After you define one or more pickup groups, assign and give each member the Call Pickup feature access code (FAC). Instead of using the Call Pickup button, users in a pickup group can dial the assigned FAC to answer calls to any other extension in their pickup group.

Procedure

1. Enter `change feature-access-codes`.
2. In the **Call Pickup Access Code** field, type the desired FAC.

   Make sure that the FAC complies with your dial plan.
3. Select **Enter** to save your changes.

Removing a user from a call pickup group

Procedure

1. Enter `change pickup-group n`, where *n* is the number of the pickup group.
2. Move to the extension that you want to remove.
3. Click **Clear** or **Delete**, depending on your system.
4. Select **Enter** to save your changes.

Deleting pickup groups

About this task

Before deleting a pickup group, you must verify if the pickup group is a member of any simple or flexible extended pickup group. If so, you must first delete the pickup group from all extended pickup groups.

Follow these three steps to delete a pickup group:

- Get a list of all extended pickup groups.
- Verify and delete the pickup group from all extended pickup groups.
- Delete the pickup group.

Getting a list of extended pickup groups

Procedure

1. Enter `list extended-pickup-group`.
2. Print this screen or write down the existing Group Numbers so that you can check each extended pickup group.
3. Click **Cancel**.

Removing a pickup group from an extended pickup group

About this task

You must remove the pickup group from all extended pickup groups.

- If your system is set up for simple extended pickup groups, the pickup group can be a member of only one extended pickup group.
- If your system is set up for flexible extended pickup groups, the pickup group can be a member of many extended pickup groups.
- If your system is set up for no extended pickup groups (none) or has no extended pickup groups assigned, you can skip this section and see *Deleting a pickup group*.

Procedure

1. Type `change extended-pickup-group n`, where `n`is the extended pickup group that you want to check.
2. Press `Enter`.
   The system displays the Extended Pickup Group screen.
3. Perform one of the following actions:
   - If the pickup group that you want to delete is not a member of this extended pickup group, Click **Cancel**.
   - If the pickup group that you want to delete is a member of this extended pickup group:
     - Select the pickup group.
     - Click **Clear** or **Delete**, depending on your system.
     - Click **Enter** to save your changes.
4. Repeat this procedure for each extended pickup group.

Deleting pickup groups

About this task

Before deleting a pickup group, you must verify if the pickup group is a member of any simple or flexible extended pickup group. If so, you must first delete the pickup group from all extended pickup groups.

Follow these three steps to delete a pickup group:

- Get a list of all extended pickup groups.
- Verify and delete the pickup group from all extended pickup groups.
- Delete the pickup group.

Getting a list of extended pickup groups

Procedure

1. Enter `list extended-pickup-group`.
2. Print this screen or write down the existing Group Numbers so that you can check each extended pickup group.
3. Click **Cancel**.

Removing a pickup group from an extended pickup group

About this task

You must remove the pickup group from all extended pickup groups.

- If your system is set up for simple extended pickup groups, the pickup group can be a member of only one extended pickup group.
- If your system is set up for flexible extended pickup groups, the pickup group can be a member of many extended pickup groups.
- If your system is set up for no extended pickup groups (none) or has no extended pickup groups assigned, you can skip this section and see *Deleting a pickup group*.

Procedure

1. Type `change extended-pickup-group n`, where `n`is the extended pickup group that you want to check.
2. Press `Enter`.
   The system displays the Extended Pickup Group screen.
3. Perform one of the following actions:
   - If the pickup group that you want to delete is not a member of this extended pickup group, Click **Cancel**.
   - If the pickup group that you want to delete is a member of this extended pickup group:
     - Select the pickup group.
     - Click **Clear** or **Delete**, depending on your system.
     - Click **Enter** to save your changes.
4. Repeat this procedure for each extended pickup group.

Deleting a pickup group

Procedure

1. Type `remove pickup-group n`, where `n` is the number of the pickup group that you want to delete.
2. Press Enter.
   The system displays the Pickup Group screen.
3. Click **Enter**.
   The system deletes the pickup group.

Related topics:

Simple extended pickup groups on page 267
Flexible Extended Pickup Groups on page 270

Changing a Call Pickup button on a user telephone

Procedure

1. Type `change station n`, where `n` is the extension that you want to change.
2. Press `Enter`.
   The system displays the Station screen.
3. Click **Next**until you see the BUTTON ASSIGNMENTS area.
4. Move to the existing **call-pkup** button.
5. Click **Clear**or **Delete**, depending on your system.
6. Move to the button number that you want to use for call pickup.
7. Type `call-pkup` after the button number.
8. Click **Enter** to save your changes.

Removing a Call Pickup button from a user telephone

Procedure

1. Enter `change station` *`n`*, where *n* is the extension that you want to change.
2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.

3. Move to the existing **call-pkup** button.
4. Click **Clear** or **Delete**, depending on your system.
5. Select **Enter** to save your changes.

Simple extended pickup groups

What if you want to have members in one pickup group be able to answer calls for another pickup group? In our example, what if you want members in the Credit Services pickup group 13 to answer calls in the Delinquency Payments pickup group 14? You can do that by setting up extended pickup groups.

If you want members of pickup group 13 to answer calls for pickup group 14, and if you want members of pickup group 14 to answer calls for pickup group 13, set your system for simple extended pickup groups.

Simple extended pickup groups allow members of two or more individual pickup groups to answer each others calls. In a simple extended pickup group, an individual pickup group can be assigned to only one extended pickup group.

All members of one pickup group can answer the calls to the other pickup groups within the simple extended pickup group.

⚠ **Caution:**

Before you administer what type of extended pickup group to use (none, simple, or flexible), be sure that your pickup group objectives are well thought out and defined.

In this exercise, you will:

- Set up the system for simple extended pickup groups.
- Assign a FAC so that users can answer calls.
- Add pickup groups, if needed
- Assign two pickup groups to an extended pickup group.

Related topics:

Adding Pickup Groups on page 260
Deleting a pickup group on page 266

Creating simple extended pickup groups

Procedure

1. Enter `change system-parameters features`.

2. Click **Next** until you see the **Extended Group Call Pickup** field.
3. In the **Extended Group Call Pickup** field, type `simple`.
4. Select `Enter` to save your changes.

Creating an extended pickup group feature access code

About this task

Users in an extended pickup group must dial an assigned FAC, followed by a 1-digit or 2-digit Pickup Numbers, to answer calls to an extension in another pickup group. Pickup groups must be in the same extended pickup group. Users cannot use a call pickup button with Extended Call Pickup.

Procedure

1. Type `change feature-access-codes`.
2. Press `Enter`.
   The system displays the Feature Access Code (FAC) screen.
3. Click **Next** until you see the **Extended Group Call Pickup Access Code** field.
4. Perform one of the following actions:
   - If the **Extended Group Call Pickup Access Code** field contains a FAC, click **Cancel**.
   - If the **Extended Group Call Pickup Access Code** field does not contain a FAC:
     - Type the desired FAC.

       Make sure that the FAC complies with your dial plan.
     - Click **Enter** to save your changes.
5. Communicate the FAC, the list of pickup numbers, and the pickup group to which each pickup number is associated, to each pickup group member who is part of the extended pickup group.

Assigning pickup groups to a simple extended pickup group

Procedure

1. Type change extended-pickup-group n, where n is a number of the extended pickup group. In this example, type change extended-pickup-group 4.

2. Press `Enter`.
   The system displays the Extended Pickup Group screen for extended pickup group 4
3. In the Pickup Group Number column, type the numbers of the pickup groups that you want to link together. In this example, add pickup group 13 (Credit Services) and pickup group 14 (Delinquency Payments).
4. Press Enter to save your changes.

Example

Pickup groups 13 and 14 are now linked together in extended pickup group 4. In addition to answering calls to their own pickup group:

- All members of pickup group 13 can answer calls to pickup group 14.
- All members of pickup group 14 can answer calls to pickup group 13.

Pickup Numbers

The **Pickup Number** column that is associated with the Pickup Group Number is the unique number that users must dial after dialing the Extended Group Call Pickup Access Code FAC to answer a call in that pickup group.

For example, let us say that the Extended Group Call Pickup Access Code FAC is *39. In the above example:

- A user in pickup group 13 must dial *391 to answer a call to pickup group 14, because pickup group 14 is assigned to Pickup Number 1.
- A user in pickup group 14 must dial *390 to answer a call to pickup group 13, because pickup group 13 is assigned to Pickup Number 0.

Note:

To minimize the number of digits that a user has to dial, first assign pickup groups to Pickup Numbers 0 to 9.

- By assigning Pickup Numbers 0 to 9, all users only needs to dial a single digit (0 to 9) after the FAC to answer the call.
- If you assign a number greater than 9 (10 to 24) to any pickup group, all users must dial two digits (00 to 24) after the FAC to answer the call.

Flexible Extended Pickup Groups

If you want members of a pickup group to answer calls for another pickup group, but you do not want the other pickup group to answer your calls, set your system for flexible extended pickup groups.

Flexible extended pickup groups still allow members of one or more individual pickup groups to answer calls of another pickup group. However, the reverse scenario is not always true. With flexible extended pickup groups, you can prevent members of one or more pickup groups from answering the calls to another pickup group.

Flexible extended pickup groups allows more control over what pickup groups can answer calls for other pickup groups. Unlike simple extended pickup groups, an individual pickup group can be in multiple flexible extended pickup groups.

The system displays the **Extended Group Number** field on the Pickup Group screen only when you set the **Extended Group Call Pickup** field on the Feature-Related System Parameters screen to flexible. When you populate the **Extended Group Number** field on the Pickup Group screen, you are associating, or "pointing," that pickup group to an extended pickup group. By pointing to an extended pickup group, members of the pickup group can answer calls made to any member of that extended pickup group.

A specific pickup group does not have to be a member of the extended pickup group that the pickup group points to. To help clarify flexible extended pickup groups, see the Example in this section.

⚠ **Caution:**

Before you administer what type of extended pickup group to use (none, simple, or flexible), be sure that your pickup group objectives are well thought out and defined.

In this exercise, you will:

- Set up the system for flexible extended pickup groups.
- Assign a FAC so that users can answer calls.
- Add or change pickup groups, and "point" a pickup group to an extended pickup group.

Related topics:

Adding Pickup Groups on page 260
Deleting a pickup group on page 266

Creating flexible extended pickup groups

Procedure

1. Type `change system-parameters features`.
2. Press `Enter`.
   The system displays the Feature-Related System Parameters screen.
3. Click **Next** until you see the **Extended Group Call Pickup** field
4. In the **Extended Group Call Pickup** field, type `flexible`.
5. Click **Enter** to save your changes.

   Your system is now set up for flexible extended pickup groups.

   To create an extended pickup group FAC, see *Creating an extended pickup group feature access code*.

Associating individual pickup groups with an extended pickup group

Procedure

1. Type `change pickup-group n`, where `n` is a pickup group number.
   In this example, let us change pickup group 15 (Executives). Type change `pickup-group 15`.
2. Press `Enter`.
   The system displays the Pickup Group screen. Notice that the system displays the **Extended Group Number** field on the Pickup Group screen. This field appears because you set the **Extended Group Call Pickup** field on the Feature-Related System Parameters screen to flexible.

   Important:

   If you change your system from simple to flexible extended pickup groups (see *Changing extended pickup groups*), the system automatically populates the **Extended Group Number** field on the Pickup Group screen for each pickup group member. For example, pickup groups 13 and 14 are members of extended pickup group 4. If you change the system from simple to flexible extended pickup groups, the system automatically populates the **Extended Group Number** field to 4 on the Pickup Group screen for these two pickup groups.

   You are not required to keep the number that the system automatically populates in the **Extended Group Number** field. You can change the number in the **Extended Group Number** field to another pickup group number. You can also make the field blank.
3. If you want to associate, or "point" the pickup group to an extended pickup group, type the number of the extended pickup group for which this pickup group can

answer calls in the **Extended Group Number** field. In this example, manually associate pickup group 15 (Executives) to extended pickup group 4. For this example, let us say that you followed the same procedure for pickup group 16 (Finance).

> **Note:**
>
> You do not have to populate the **Extended Group Number** field. You can leave the **Extended Group Number** field blank. You can just as easily point the pickup group to a different extended pickup group. For example, you can point pickup group 13 (Credit Services) to extended pickup group 2, even though pickup group 13 is not a member of extended pickup group 2.

4. Click **Enter** to save your changes.

Assigning pickup groups to a flexible extended pickup group

Procedure

1. Type `change extended-pickup-group n`, where `n` is the number of the extended pickup group.
   In this example, type `change extended-pickup-group`.
2. Press `Enter`.
   The system displays the Extended Pickup Group screen for extended pickup group 4
3. Add pickup group 16 (Finance) to this extended pickup group.
4. Click **Enter** to save your changes.

Example

Here is how flexible extended pickup groups work.

Notice that pickup groups 13, 14, and 16 are now members of extended pickup group 4. On the Pickup Group screen for pickup groups 13, 14, and 16, you also pointed each pickup group to extended pickup group 4.

Pickup group 15 (Executives) is not a member of extended pickup group 4. However, on the Pickup Group screen for group 15 (Figure 96: Pickup Group screen on page 266), you pointed pickup group 15 to extended pickup group 4.

In addition to answering calls to their own pickup group:

Notice that pickup groups 13, 14, and 16 are now members of extended pickup group 4. On the Pickup Group screen for pickup groups 13, 14, and 16, you also pointed each pickup group to extended pickup group 4.

Pickup group 15 (Executives) is not a member of extended pickup group 4. However, on the Pickup Group screen for group 15 (Figure 96), you pointed pickup group 15 to extended pickup group 4.

In addition to answering calls to their own pickup group:

- Any member of pickup group 13 can answer calls to pickup groups 14 and 16.
- Any member of pickup group 14 can answer calls to pickup groups 13 and 16.
- Any member of pickup group 16 can answer calls to pickup groups 13 and 14.
- Any member of pickup group 15 can answer calls to pickup groups 13, 14, and 16 because pickup group 15 points to extended pickup group 4.
- Any member of pickup groups 13, 14 and 16 cannot answer calls to pickup group 15 because pickup group 15 is not a member of extended pickup group 4.

Changing extended pickup groups

About this task

You define extended pickup groups on a system-wide basis. The system cannot support both simple and flexible extended pickup groups at the same time. You can, however, change your extended pickup groups from one type to another.

Related topics:

Call Pickup on page 257
Simple extended pickup groups on page 267
Flexible Extended Pickup Groups on page 270
Directed Call Pickup on page 274

Changing from simple to flexible

About this task

If you want to change all extended pickup groups from simple to flexible, you can easily make the change. See *Creating flexible extended pickup groups*. The system automatically populates the **Extended Group Number** field on the Pickup Group screen for all pickup groups that are part of an extended pickup group.

Changing from flexible to simple

About this task

The process is more complex to change all extended pickup groups from flexible to simple. Before you can change the extended pickup group from flexible to simple, you must first delete all of the individual pickup groups from all of the extended pickup groups. Then you can change the extended pickup group from flexible to simple (see *Creating simple extended pickup groups*). After that step, you must re-administer all of the extended pickup groups again.

Directed Call Pickup

If you do not want to set up pickup groups and extended pickup groups, but still want selected people to answer other telephones, use Directed Call Pickup. Before a person can use this feature, you must enable Directed Call Pickup on your system.

- Telephones that can be answered by another extension using Directed Call Pickup must have a Class of Restriction (COR) that allows this feature.
- Telephones that can answer another extension using Directed Call Pickup must have a COR that allows this feature.

In this exercise, you will:

- Determine if Directed Call Pickup is enabled on your system.
- Create one or more Classes of Restriction (COR) that allow Directed Call Pickup.
- Assign the COR to individual extensions.
- Assign a Directed Call Pickup button to each extension that is assigned the COR.
- Assign a feature access code (FAC).

Ensuring Directed Call Pickup availability

About this task

Before you can assign Directed Call Pickup to a user, you must ensure that Directed Call Pickup is available on your system.

Procedure

1. Type `change system-parameters features`.
2. Press `Enter`.
   The system displays the Feature-Related System Parameters screen.
3. Click **Next** until you see the **Directed Call Pickup?** field
4. Perform one of the following actions:
   a. If the **Directed Call Pickup?** field is set to y, your system is set up for Directed Call Pickup. Click **Cancel**.
   b. If the **Directed Call Pickup?** field is set to n:
      - Type `y` in the field.
      - Click **Enter** to save your changes.

Creating Classes of Restriction for Directed Call Pickup

About this task

You must create one or more Classes of Restriction (COR) that allow Directed Call Pickup. All users to whom you assign a COR can then use Directed Call Pickup.

There are three ways to set up a COR for Directed Call Pickup. You can create a COR where users can:

- Only have their extensions answered by Directed Call Pickup. Users with this COR cannot pick up other extensions.
- Only pick up other extensions using Directed Call Pickup. Users with this COR cannot have their extensions answered by other users.
- Both have their extensions answered by Directed Call Pickup and pick up other extensions.

Procedure

1. Enter `change COR` *`n`*, where *n* is the COR that you want to change.
2. Perform one of the following actions:
   a. To create one or more CORs where the extensions can only be picked up by the Directed Call Pickup feature, but not be able to pick up other extensions:
      - Type `y` in the **Can Be Picked Up By Directed Call Pickup** field.
      - Leave the **Can Use Directed Call Pickup** field set to `n`.

        Any extension to which you assign this COR can only be picked up by the Directed Call Pickup feature.

   b. To create one or more CORs where the extensions can only use the Directed Call Pickup feature to pick up other extensions, but not be picked up by other extensions:
      - Leave the **Can Be Picked Up By Directed Call Pickup** field set to `n`.
      - Type `y` in the **Can Use Directed Call Pickup** field.

        Any extension to which you assign this COR can only use the Directed Call Pickup feature to pick up other extensions.

   c. To create one or more CORs where the extensions can use the Directed Call Pickup feature both to pick up other extensions and be picked up by other extensions:
      - Type `y` in the **Can Be Picked Up By Directed Call Pickup** field.
      - Type `y` in the **Can Use Directed Call Pickup** field.

Any extension to which you assign this COR can use the Directed Call Pickup feature both to pick up other extensions and be picked up by other extensions.

3. Select **Enter** to save your changes.

Assigning a Class of Restriction to a user

About this task

You must assign a COR to user extensions before anyone can use Directed Call Pickup.

Procedure

1. Enter `change station n`, where *n* is the extension that you want to change.
2. In the **COR** field, type the appropriate COR that allows Directed Call Pickup capabilities.
3. Select **Enter** to save your changes.

Assigning a Directed Call Pickup button

About this task

Assign a Directed Call Pickup button to all extensions that share a COR where the **Can Use Directed Call Pickup** field is set to y.

Procedure

1. Enter `change station n`, where *n* is an extension to which you have assigned the Directed Call Pickup COR.
2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
3. Move to the button number that you want to use for Directed Call Pickup. You can use any of the available buttons.
4. Type `dir-pkup` after the button number.
5. Select **Enter** to save your changes.

   Repeat this procedure for each member of the COR who can pick up other extensions using Directed Call Pickup.

Assigning a Directed Call Pickup feature access code

About this task

Also assign a Directed Call Pickup feature access code (FAC). Give the FAC to each user whose extension shares a **COR where the Can Use Directed Call Pickup** field is set to y.

Instead of using the Directed Call Pickup button, users can dial the assigned FAC to answer calls using Directed Call Pickup.

Procedure

1. Enter `change feature-access-codes`.
2. Click **Next** until you see the **Directed Call Pickup Access Code** field.
3. Perform one of the following actions:
    a. If the **Directed Call Pickup Access Code** field already contains a code, click **Cancel**.
    b. If the **Directed Call Pickup Access Code** field does not contain a code:
        - Type a code in the field. Make sure that the code you type conforms to your dial plan.
        - Select **Enter** to save your change.

    Communicate the FAC with each member of the COR that can pick up other extensions using Directed Call Pickup.

Removing Directed Call Pickup from a user

Procedure

1. Enter`change station` *`n`*, where *n* is the extension of the user.
2. In the **COR** field, type a different COR that does not have Directed Call Pickup permissions.
3. Click **Next** until you see the **BUTTON ASSIGNMENTS** section.
4. Move to the button number that contains dir-pkup.
5. Click **Clear** or **Delete**, depending on your system.
6. Select **Enter** to save your changes.

Hunt Groups

A hunt group is a group of extensions that receive calls according to the call distribution method you choose. When a call is made to a certain telephone number, the system connects the call to an extension in the group.

Use hunt groups when you want more than one person to be able to answer calls to the same number. For example, set up a hunt group for:

- a benefits department within your company
- a travel reservations service

Setting up hunt groups

About this task

Let us set up a hunt group for an internal helpline. Before making changes to Communication Manager, we'll decide:

- the telephone number for the hunt group
- the number of people answering calls
- the way calls are answered

Our dial plan allows 4-digit internal numbers that begin with 1. The number 1200 is not in use. So, we'll set up a helpline hunt group so anyone within the company can call extension 1200 for help with a telephone.

We will assign 3 people (agents) and their extensions to our helpline. We want calls to go to the first available person.

Procedure

1. Type `add hunt-group next`.
2. Press `Enter`.
   The system displays the Hunt Group screen. The **Group Number** field is automatically filled in with the next hunt group number.
3. In the **Group Name** field, type the name of the group.
   In our example, type `internal helpline`.
4. In the **Group Extension** field, type the telephone number.
   We'll type `1200`.
5. In the **Group Type** field, type the code for the call distribution method you choose.

We'll type `ucd-loa` so a call goes to the agent with the lowest percentage of work time since login.

> **Note:**
>
> The COS for all hunt groups defaults to 1. Therefore, any changes to COS 1 on the Class of Service screen changes the COS for all your hunt groups. A **COS** field does not appear on the Hunt Group screen.

6. Click **Next Page** to find the Group Member Assignments screen.
7. In the **Ext** field, type the extensions of the agents you want in the hunt group. We'll type `1011`, `1012`, and `1013`.

   > **Tip:**
   >
   > For a ddc group type (also known as "hot seat" selection), the call is sent to the extension listed in the first **Ext** field. The system uses this screen to determine the hunting sequence.

8. Click **Enter** to save your changes.

   The **Name** fields are display-only and do not appear until the next time you access this hunt group.

Dynamic hunt group queue slot allocation

The dynamic hunt group queue slot allocation feature eliminates the need to preallocate queue slots for hunt groups. The system dynamically allocates the queue slots from a common pool on an as-needed basis. All possible calls can be queued. There is no additional administration needed. This feature expands the capacities of your system by eliminating the potential of missed calls due to a full queue

When the **Queue?** field on the Hunt Group screen is set to y, this feature applies to all uses of hunt groups:

- Automatic Call Distribution (ACD) non-vector/vector splits and skills
- Non-ACD hunt group
- Voice mail

Changing a hunt group

Procedure

1. Enter `change hunt-group` *`n`*, where *n* is the number of the hunt group.
2. Change the necessary fields.

3. Select **Enter** to save your changes.

Setting up a queue

About this task

You can tell your server running Communication Manager how to handle a hunt-group call when it cannot be answered right away. The call waits in "queue."

We will tell Communication Manager that as many as 10 calls can wait in the queue, but that you want to be notified if a call waits for more than 30 seconds.

You also want Communication Manager to send a warning when 5 or more calls are waiting in the queue. This warning flashes queue-status buttons on telephones that have a status button for this hunt group. When the buttons flash, everyone answering these calls can see that the help-line calls need more attention.

Procedure

1. Type `change hunt-group n`, where `n` is the number of the hunt group to change.
2. Press `Enter`.
   In our example, type `change hunt-group 5`.

   The system displays the Hunt Group screen.
3. In the **Queue** field, type `y`.
4. In the **Queue Length** field, type the maximum number of calls that you want to wait in the queue.
   In our example, type `10`.
5. In the **Calls Waiting Threshold** field, type the maximum number of calls that can be in the queue before the system flashes the queue status buttons.
   In our example, type `5`.
6. In the **Time Warning Threshold** field, type the maximum number of seconds you want a call to wait in the queue before the system flashes the queue status buttons.
   In our example, type `30`.
7. Click **Enter** to save your changes.

Hunt groups for TTY callers

Several laws, such as the Americans with Disabilities Act (ADA) of 1990 and Section 255 of the Telecommunications Act of 1996, require that“ reasonable accommodation” be provided for people with disabilities. For this reason, your company might choose to offer support for callers who use TTYs. (These devices are also known as TDDs -- “Telecommunication Device for the Deaf” -- but the term TTY is generally preferred, in part because many users of these devices are hearing-impaired, but not deaf.)

TTY callers can be accommodated by creating a hunt group that includes TTY-equipped agents. The TTY itself looks a little like a laptop computer, except that it has a one- or two-line alphanumeric display instead of a computer screen. The cost of a typical TTY is approximately three hundred dollars. Although many TTYs can connect directly with the telephone network via analog RJ-11 jacks, Avaya recommends that agents be equipped with TTYs that include an acoustic coupler that can accommodate a standard telephone handset. One reason for this recommendation is that a large proportion of TTY users are hearing impaired, but still speak clearly. These individuals often prefer to receive calls on their TTYs and then speak in response. This requires the call center agent to alternate between listening on the telephone and then typing on the TTY, a process made considerably easier with an acoustically coupled configuration.

Although TTY-emulation software packages are available for PCs, most of these do not have the ability to intermix voice and TTY on the same call.

For a TTY hunt group, you can record TTY announcements and use them for the hunt group queue. To record announcements for TTY, simply follow the same steps as with voice recordings from your telephone (see *Managing Announcements*). However, instead of speaking into your telephone to record, you type the announcement with the TTY device.

Note:

For an alternative to simply creating a TTY hunt group, you can use vectors to process TTY calls. With vectors, you can allow TTY callers and voice callers to use the same telephone number. In this case, you can also record a single announcement that contains both TTY signaling and a voice recording.

Adding hunt group announcements

About this task

You can add recorded announcements to a hunt group queue. Use announcements to encourage callers to stay on the line or to provide callers with information. You can define how long a call remains in the queue before the caller hears an announcement.

For more information on how to record an announcement, see “Announcements” in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Let us add an announcement to our internal helpline. We want the caller to hear an announcement after 20 seconds in the queue, or after approximately 4 or 5 rings. Our announcement is already recorded and assigned to extension 1234.

Tip:

You can use `display announcements` to find the extensions of your recorded announcements.

Procedure

1. Type `change hunt-group n`, where `n` is the number of the hunt group to change.
2. Press `Enter`.
   In our example, type `change hunt-group 5`.

   The system displays the Hunt Group screen.
3. Click **Next Page** to find the **First Announcement Extension** field.
4. In the **First Announcement Extension** field, type the extension of the announcement you want callers to hear.
   In this example, type `1234`.
5. In the **First Announcement Delay (sec)** field, type the number of seconds you want the caller to wait before hearing the first announcement.
   In our example, type `20`.

   Tip:

   If you set the delay announcement interval to 0, callers automatically hear the announcement before anything else. This is called a “forced first announcement.”
6. Click **Enter** to save your changes.

   You can use the same announcement for more than one hunt group.

Vectors and VDNs

This section provides an introduction to vectors and Vector Directory Numbers (VDN). It gives you basic instructions for writing simple vectors.

Security alert:

Vector fraud is one of the most common types of toll fraud because vectors route calls based on the Class of Restriction (COR) assigned to the VDN. See *BCS Products Security Handbook, 555-025-600* for more information.

This section references announcements, hunt groups, queues, splits, and skills, which are covered in detail in other sections of this book. You can also find information about these topics in *Avaya Call Center Call Vectoring and Expert Agent Selection (EAS) Guide, 07-600780*.

Note:

The **Client Room** field on the Class of Service screen will affect VDN displays. If a local station that has a COS with the **Client Room** field set to y calls a local VDN, the agent's display that receives the call will look as if it is a direct station call rather than the expected VDN display of "station name to vdn name."

What are Vectors?

A vector is a series of commands that you design to tell the system how to handle incoming calls. A vector can contain up to 32 steps and allows customized and personalized call routing and treatment. Use call vectoring to:

- play multiple announcements
- route calls to internal and external destinations
- collect and respond to dialed information

Tip:

The vector follows the commands in each step in order. The vector "reads" the step and follows the command if the conditions are correct. If the command cannot be followed, the vector skips the step and reads the next step.

Your system can handle calls based on a number of conditions, including the number of calls in a queue, how long a call has been waiting, the time of day, day of the week, and changes in call traffic or staffing conditions.

Putting a call in a queue

About this task

Write a vector so that calls that come into the main business number redirect to a queue.

We will use a vector-controlled hunt group for the main number queue. This hunt group was set up as main split 47. When calls first arrive, all calls to our main number should be queued as "pri 1" for low priority.

To queue calls, write the following vector (step 2). (Please note, we started our example on step 2 because step 1 is used later.)

Procedure

1. Keep it Blank.
2. Type `queue-to main split 47 pri 1`.

Tip:

Remember, Communication Manager automatically fills in some of the information when you type your vector step. Press `Tab`.

Playing an Announcement

About this task

Write a vector to play an announcement for callers in a queue. Use the announcement to ask callers to wait. You need to record the announcement before the vector can use it.

Let us play our announcement 4001, asking the caller to wait, then play music for 60 seconds, then repeat the announcement and music until the call is answered. The goto command creates the loop to repeat the announcement and the music. Unconditionally means under all conditions.

Tip:

Rather than loop your vectors directly back to the announcement step, go to the previous queue-to step. This way, if for some reason the call does not queue the first time, Communication Manager can attempt to queue the call again. If the call successfully queued the first time though, it merely skips the queue-to step and plays the announcement. The system cannot queue a call more than once in the exact same priority level.

To play and repeat an announcement, write this vector (steps 3-5):

Procedure

1. Keep it Blank.
2. Type `queue-to main split 47 pri 1`.
3. Type `announcement 4001 (All agents are busy, please wait...)`.
4. Type `wait-time 60 secs hearing music`.
5. Type `goto step 2 if unconditionally`.

Routing Based On Time Of Day

About this task

Write a vector for calls that come in after your office closes.

Assume that your business is open 7 days a week, from 8:00 a.m. to 5:00 p.m. When calls come in after business hours, you want to play your announcement 4002, which states that the office is closed and asks callers to call back during normal hours. Write the vector so the call disconnects after the announcement is played.

For after hours treatment, write this vector (steps 1, 6, and 7):

Procedure

1. Type `goto step 7 if time-of-day is all 17:00 to all 8:00`.
2. Type `queue-to main split 47 pri 1`.
3. Type `announcement 4001 (All agents are busy, please wait...)`.
4. Type `wait-time 60 secs hearing music`.
5. Type `goto step 2 if unconditionally`.
6. Type `stop`.
7. Type `disconnect after announcement 4002 ("We're sorry, our office is closed...")`.

   If the `goto` command in step 5 fails, Communication Manager goes to the next step. The `stop` in step 6 prevents callers from incorrectly hearing the “office is closed” announcement in step 7. `Stop` keeps the call in the state it was in before the command failed. In this case, if step 5 fails, the call remains in step 4 and the caller continues to hear music.

   ⚠ Caution:

   Add a stop vector step only after calls are routed to a queue. If a stop vector is executed for a call not in queue, the call drops.

Allowing callers to leave a message

About this task

Write a vector that allows callers to leave messages. This type of vector uses a hunt group called a messaging split. For our example, we send after-hours calls to the voice mailbox at extension 2000 and use messaging split 99.

Once the vector routes a call to the mailbox, the caller hears a greeting (that was recorded with the voice mail for mailbox 2000) that tells them they can leave a message.

To let callers leave messages, write this vector (step 7):

Procedure

1. Type `goto step 7 if time-of-day is all 17:00 to all 8:00`.
2. Type `queue-to main split 47 pri 1`.
3. Type `announcement 4001 (All agents are busy, please wait...)`.

4. Type `wait-time 60 secs hearing music`.
5. Type `goto step 2 if unconditionally`.
6. Type `stop`.
7. Type `messaging split 99 for extension 2000`.

Redirecting calls during an emergency or holiday

About this task

You can provide a quick way for a supervisor or agent to redirect calls during an emergency or holiday. Use a special mailbox where you can easily change announcements. This vector is also an alternative to making sure all agents log out before leaving their telephones.

In our example, no agents are normally logged in to split 10. We'll use split 10 for an emergency. We preset buttons on our agents' telephones so people with these telephones can log in at the touch of a button.

To quickly redirect calls:

Create a special mailbox with the appropriate announcement such as “We are unable to answer your call at this time” or "“Today is a holiday, please call back tomorrow.”

In our example, we recorded the mailbox greeting for extension 2001.

Insert the following steps (steps 1, 10, and 11).

See *Inserting a step*.

Procedure

1. Type `goto step 10 if staff agents split 10 > 0`.
2. Type `goto step 8 if time-of-day is all 17:00 to all 8:00`.
3. Type `queue-to main split 47 pri 1`.
4. Type `announcement 4001 (All agents are busy, please wait...)`.
5. Type `wait-time 60 secs hearing music`.
6. Type `goto step 2 if unconditionally`.
7. Type `stop`.
8. Type `messaging split 99 for extension 2000`.
9. Type `stop`.
10. Type `messaging split 99 for extension 2001`.
11. Type `stop`.

    When there is an emergency, fire drill, or holiday, the supervisor or agent logs into this split. When an agent logs into split 10, the system looks at vector step 1, sees that more than 0 people are logged into split 10, and sends calls to step 10 (which sends to messaging split 99). When your business returns to normal and the agent logs out of split 10, call handling returns to normal.

Giving callers additional choices

About this task

You can give your callers a list of options when they call. Your vector tells Communication Manager to play an announcement that contains the choices. Communication Manager collects the digits the caller dials in response to the announcement and routes the call accordingly.

We'll create a vector that plays an announcement, then lets callers dial an extension or wait in the queue for an attendant.

Please note, the following example of this "auto attendant" vector is a new vector and is not built on the vector we used in the previous example.

To let callers connect to an extension, write this kind of vector:

Procedure

1. Type `wait-time 0 seconds hearing music`.
2. Type `collect 4 digits after announcement 4004 (You have reached our company. Please dial a 4-digit extension or wait for the attendant.)`.
3. Type `route-to digits with coverage y`.
4. Type `route-to number 0 with cov n if unconditionally`.
5. Type `stop`.

Inserting a Step

About this task

It is easy to change a vector step and not have to retype the entire vector. We will add announcement 4005 between step 3 and step 4 in vector 20.

Procedure

1. Type `change vector 20`. Press `Enter`.
   The system displays the Call Vector screen.
2. Click **Edit**.

3. Type `i` followed by a space and the number of the step you want to add.
   In our example, type `i 4`.
4. Type the new vector step.
   We will type `announcement 4005 (Please wait...).`
5. Click **Enter** to save your changes.

   ⊕ **Tip:**

   When you insert a new vector step, the system automatically renumbers the rest of the vector steps and all references to the vector steps. Communication Manager inserts a “*” when the numbering needs more attention.

Deleting a Step

Procedure

1. Type `change vector 20`. Press `Enter`.
   The system displays the Call Vector screen.
2. Click **Edit**.
3. Type `d` followed by a space and the number of the step you want to delete.
   In our example, type `d 5`.

   ⊕ **Tip:**

   You can delete a range of vector steps. For example, to delete steps 2 through 5, type `d 2-5`. Click **Enter**.
4. Click **Enter** to save your changes.

   ⊕ **Tip:**

   When you delete a vector step, the system automatically renumbers the rest of the vector steps and all references to the vector steps. An asterisk (*) is inserted when the numbering needs more attention.

Variables in Vectors

Variables in Vectors (VIV) is a Call Vectoring feature that allows you to create variables that can be used in vector commands to:

- Improve the general efficiency of vector administration
- Provide increased manager and application control over call treatments
- Allow you to create more flexible vectors that better serve the needs of your customer and contact center operations

The vector variables are defined in a central variable administration table. Values assigned to some types of variables can also be quickly changed by means of special vectors, Vector Directory Numbers (VDNs), or Feature Access Codes (FACs) that you administer specifically for that purpose. Different types of variables are available to meet different types of call processing needs. Vector variables can be added to “consider location,”“messaging,” and "“adjunct routing” vector steps when the Call Center Release is 3.0 or later. Depending on the variable type, variables can use either call-specific data or fixed values that are identical for all calls. In either case, an administered variable can be reused in many vectors. For a more detailed description of variable types and purposes, see *Avaya Call Center Call Vectoring and Expert Agent Selection (EAS) Guide, 07-600780*.

Administering Vector Variables

About this task

Administering variables and implementing them in your vectors is a relatively simple process:

Procedure

1. First, determine how you intend to use the new variable and identify its defining characteristics. Use this information to decide on an available variable type that meets your needs.
2. Type `change variables`.
   The Variables for Vectors screen appears.
3. In the **Var** column, select an unused letter between A and Z. This letter is used to represent this variable in vector steps. Complete the editable fields in the row that you select. Depending on your entry in the **Type** field, some fields in the row may be pre-populated and display-only, or not applicable.
   - **Description** - a short description of your variable
   - **Type** - the variable type
   - **Scope** - local or global
   - **Length** - length of the digit string
   - **Start** - digit start position
   - **Assignment** - pre-assigned value
   - **VAC** - Variable Access Code (for value variable type only)

4. Click **Enter** to save your changes.

Handling TTY calls with vectors

About this task

Unlike fax machines and computer modems, a Tele-typewriter device (TTY) has no handshake tone and no carrier tone. A TTY is silent when not transmitting. This is why systems cannot identify TTY callers automatically. However, the absence of these special tones also means that voice and TTY tones can be intermixed in pre-recorded announcements. The ability to provide a hybrid voice-and-TTY announcement, when combined with the auto-attendant vectoring capability, can permit a single telephone number to accommodate both voice and TTY callers.

The sample vector that follows allows TTY callers to access a TTY agent. It begins with a step that plays a TTY announcement combined with a voice announcement. The announcement tells the TTY caller to enter a digit that will direct them to a TTY support person. The vector then processes the digit entered to connect the TTY caller to the TTY split (or hunt group). For more information on recording TTY announcements, see *Managing Announcements*.

In the following example, split 47 (hunt group 47) has already been established and consists of TTY-enabled agents.

If a TTY caller calls the number that connects to vector 33, the following occurs:

Procedure

1. After a short burst of ringing, a quick burst of TTY tones is sent to the caller telling the caller to hold, “HD”. Then, a voice announcement follows for callers using a normal telephone connection. The announcement tells them to stay on the line. Finally, another burst of TTY tones is sent to the TTY caller which displays on the caller’s TTY device as,“Dial 1.” The TTY caller won’t hear the voice announcement, but because the step collects digits, it allows the caller to enter `1` on his or her touchtone telephone.

   Note:

   For voice callers, the burst of TTY tones lasts about one second and sounds like a bird chirping.

2. In vector step 3, since the TTY caller entered `1` in vector step 2, the TTY caller is sent to vector step 8, at which point the caller is put in queue for a TTY-enabled agent in split 47.

   Note:

   The voice caller is sent to vector step 3 also, but a voice caller does not go to vector step 8 because the caller did not enter `1` at vector step 2. Instead, voice callers continue on to vector step 4, where they connect to split 48.

3. While the TTY caller waits in queue, he or she hears silence from vector step 9, then the announcement in vector step 10, and is then looped back to wait with silence by vector step 11.

   See the *Avaya Call Center Call Vectoring and Expert Agent Selection (EAS) Guide, 07-600780*, for more information.

   Automated Attendant competes with several features for ports on the Call Classifier — Detector circuit pack or equivalent. See the*Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207 for more information on the circuit pack.

Fixing vector problems

About this task

If there is a problem with a vector, Communication Manager records the error as a vector event. Vector events occur for a number of reasons including problems with a trunk, full queue slots, or the vector reaching the maximum 1000 steps allowed.

Use `display events` to access the Event Report screen and see the event record. Use the event record to see why the vector failed.

To view the Event Report:

Procedure

1. Type `display events`.
2. Press `Enter`.
   The system displays the Event Report screen.
3. To see all current vector events, click**Enter**.
   OR

   Indicate the events that you want to see by completing the **Report Period** and **Search Option** fields.
4. Click **Enter** to view the report.
   The system displays the Event Report (detail) screen.

   Look at the information in the **Event Data** field to diagnose the vector event. In this example, there was a problem with:

   - Vector 12, step 5
   - Split 89

Vector Directory Numbers

A VDN is an extension that directs an incoming call to a specific vector. This number is a "soft" extension number not assigned to an equipment location. VDNs must follow your dial plan.

We will create VDN 5011 for our sales department. A call into 5011 routes to vector 11. This vector plays an announcement and queues calls to the sales department.

Security alert:

Vector fraud is one of the most common types of toll fraud because vectors route calls based on the class of restriction (COR) assigned to the VDN. See the *Avaya Toll Fraud and Security Handbook*, 555-025-600 for more information.

Adding a vector directory number

Procedure

1. Type `add VDN 5011`.
2. Press `Enter`.
3. You enter the VDN extension you want to add.
   The system displays the Vector Directory Number screen.
4. Type a description for this VDN in the **Name** field.
   In our example, type `Sales Department`.

   The information in the VDN Name field appears on a display telephone. This allows the agent to recognize the nature of the call and respond accordingly.

   Tip:

   The **VDN Override** on the Vector Directory Number screen controls the operation of the display.
5. Enter the vector number.
   In our example, type `11`.
6. In the **Measured** field, indicate how you want to measure calls to his VDN.
   In our example, type `both` (for both CMS and BCMS).

   Tip:

   BCMS must be enabled to use both. Use `display system-parameters customer-options` to see if BCMS is enabled.
7. Click **Enter** to save your changes.

Viewing vector directory numbers

Procedure

1. Type `list VDN`.
2. Press `Enter`.
   The system displays the Vector Directory Number screen.
3. Each VDN maps to one vector. Several VDNs can map to the same vector.

Automatic Call Distribution

Automatic Call Distribution (ACD) is an Avaya Communication Manager feature used in many contact centers. ACD gives you greater flexibility to control call flow and to measure the performance of agents.

ACD systems operate differently from non-ACD systems, and they can be much more complex. ACD systems can also be more powerful because they allow you to use features and products that are not available in non-ACD systems. See the *Avaya Call Center Release 4.0 Automatic Call Distribution (ACD) Guide, 07-600779*, for more information on ACD call centers.

ACD System Enhancement

First, all call center management systems (such as Avaya's Basic Call Management System (BCMS), BCMSVu, and the sophisticated Avaya IP Agent Call Management System) require ACD. These management systems give you the ability to measure more aspects of your center's operation, and in more detail, than is possible with standard Avaya Communication Manager reports.

Call vectoring greatly enhances the flexibility of a call center, and most vectoring functions require ACD. Vectoring is a simple programming language that allows you to custom design every aspect of call processing.

Together, ACD and vectoring allow you to use Expert Agent Selection (EAS) For a variety of reasons, you might want certain agents to handle specific types of calls. For example, you might want only your most experienced agents to handle your most important customers. You might have multilingual agents who can serve callers in a variety of languages.

EAS allows you to classify agents according to their specific skills and then to rank them by ability or experience within each skill. Avaya Communication Manager uses these classifications to match each call with the best available agent. See *Avaya Call Center Call*

Vectoring and Expert Agent Selection (EAS) Guide, 07-600780, for more information on call vectoring and EAS.

Assigning a Terminating Extension Group

About this task

A Terminating Extension Group (TEG) allows an incoming call to ring as many as 4 telephones at one time. Any user in the group can answer the call.

Once a member of the TEG has answered a group call, the TEG is considered busy. If a second call is directed to the group, it follows a coverage path if one has been assigned.

The following example shows how to assign a terminating extension group to the advertising department.

For example, we will assign this TEG to extension 6725.

Procedure

1. Type `add term-ext-group next`.
2. Press `Enter`.
   The system displays the Terminating Extension Group screen.
3. In the **Group Extension** field, type `6725`.

   This is the extension for the advertising group.
4. In the **Group Name** field, type `advertising`.

   This is the name of the group.
5. In the **Coverage Path** field, type `5`.

   This is the number of the call coverage path for this group.

Chapter 11: Routing Outgoing Calls

World Class Routing

Your system uses Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) to direct outgoing calls.

- AAR routes calls within your company over your own private network.
- ARS routes calls that go outside your company over public networks. ARS also routes calls to remote company locations if you do not have a private network.

Automatic routing begins when a user dials a feature access code (FAC) followed by the number the user wants to call. Avaya Communication Manager analyzes the digits dialed, selects the route for the call, deletes and inserts digits if necessary, and routes the call over the trunks you specify in your routing tables. ARS and AAR can access the same trunk groups and share the same route patterns and other routing information. ARS calls can be converted to AAR calls and vice-versa.

The FAC for AAR is usually the digit 8. The FAC for ARS is usually the digit 9 in the US and 0 outside of the US. Your Avaya technician or business partner sets up AAR on your server running Communication Manager and usually assigns the AAR FAC at the same time. You can administer your own ARS FAC.

This section describes only ARS call routing.

Calling Privileges Management

Each time you set up a telephone, you use the Station screen to assign a class of restriction (COR). You can create different CORs for different groups of users. For example, you might want executives in your company to have different calling privileges than receptionists.

When you set up a COR, you specify a Facility Restriction Level (FCL) on the Class of Restriction screen. The FRL determines the calling privileges of the user. Facility Restriction Levels are ranked from 0–7, where 7 has the highest level of privileges.

You also assign an FRL to each route pattern preference in the Route Pattern screen. When a user makes a call, the system checks the user’s COR. The call is allowed if the caller’s FRL is higher than or equal to the route pattern preference’s FRL.

Changing Station

About this task

Let us say we are setting up a new telephone for an executive. The current translations assign COR 1, with outward restrictions and an FRL 0, which is the lowest permission level available. We want to assign a COR with the highest level of permissions, FRL 7, to station 1234.

To change station 1234 from COR 1 to COR 7:

Procedure

1. Type `change station 1234`.
2. Press **Enter**.
   The Station screen appears.
3. In the **COR** field, type `7`.
4. Press `Enter` to save your changes.
5. To change from FRL 0 to FRL 7, type `change cor 7`.
6. Press **Enter**.
   The Class of Restriction screen appears.
7. In the **FRL** field, type `7`.
8. Press **Enter** to save your changes.
   Now all users with COR 7 will have the highest level of calling permissions.

Assigning ARS FAC

Before you begin

Be sure the ARS feature access code (FAC) is set up on your system. In the U.S., 9 is usually the ARS FAC. Users dial 9 to make an outgoing call.

About this task

When a user dials 9 to access ARS and make an outgoing call, the ARS access code 9 is dropped before digit analysis takes place. will not be part of the digit analysis.

To assign the ARS FAC:

Procedure

1. Type `change dialplan`.

2. Press **Enter**.
   The DCS to QSIG TSC Gateway appears.
3. Move to the 9 row and type `fac` in the first column.
4. Press `Enter` to save your changes.
5. Type `change features`.
6. Press **Enter**.
   The Feature Access Code (FAC) screen appears.
7. Type `9` in the **ARS - access code** field.
8. Press **Enter** to save your changes.

Location ARS FAC

The **Location ARS FAC** allows users in different locations to use the same “culturally significant” FAC they are accustomed to, such as dialing 9 for an outside line, and access the same feature. The Location ARS FAC is only accessible for calling numbers at locations administered with that ARS FAC (for details on setting up Location ARS FAC, see the Locations screen). If an attempt is made to use an ARS FAC at a location for which it is not valid, the attempt is denied. The ARS access code on the Feature Access Code (FAC) screen continues to be used when a location ARS does not exist. If a location ARS FAC exists, then the ARS access code on the Feature Access Code (FAC) screen is prohibited/denied from that location.

By using a local ARS code, the ability to administer two ARS codes on the Feature Access Code (FAC) screen is lost.

Displaying ARS Analysis Information

About this task

You will want to become familiar with how your system currently routes outgoing calls. To display the ARS Digit Analysis Table that controls how the system routes calls that begin with 1:

Procedure

1. Type `display ars analysis 1`.
2. Press `Enter` .
   The ARS Digit Analysis Table for dialed strings that begin with 1 appears.

Note:

Communication Manager displays only as many dialed strings as can fit on one screen at a time.

Note:

Type `display ars analysis` and press `Enter` to display an all-location screen. For details on command options, see online help, or *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

3. To see all the dialed strings that are defined for your system, run an ARS Digit Analysis report:

   a. Type `list ars analysis`.

   b. Press **Enter**.
      The ARS Digit Analysis Report appears.

   You might want to print this report to keep in your paper records.

ARS Analysis

With ARS, Communication Manager checks the digits in the number called against the ARS Digit Analysis Table to determine how to handle the dialed digits. Communication Manager also uses Class of Restriction (COR) and Facility Restriction Level (FRL) to determine the calling privileges.

Let us look at a very simple AAR and ARS digit analysis table. Your system likely has more defined dialed strings than this example.

The far-left column of the ARS Digit Analysis Table lists the first digits in the dialed string. When a user makes an outgoing call, the system analyzes the digits, looks for a match in the table, and uses the information in the matching row to determine how to route the call.

Let us say a caller places a call to 1-303-233-1000. Communication Manager matches the dialed digits with those in the first column of the table. In this example, the dialed string matches the “1”. Then Communication Manager matches the length of the entire dialed string (11 digits) to the minimum and maximum length columns. In our example, the 11-digit call that started with 1 follows route pattern 30 as an fnpa call.

Tip:

The first dialed digit for an external call is often an access code. If ‘9’ is defined as the ARS access code,Communication Manager drops this digit and analyzes the remaining digits with the ARS Analysis Table.

The Route Pattern points to the route that handles the calls that match this dial string. **Call Type** tells what kind of call is made with this dial string.

Call type helps Communication Manager decide how to handle the dialed string.

Examples Of Digit Conversion

Purpose

Your system uses the AAR or ARS Digit Conversion Table to change a dialed number for more efficient routing. Digits can be inserted or deleted from the dialed number. For instance, you can tell Communication Manager to delete a 1 and an area code on calls to one of your locations, and avoid long-distance charges by routing the call over your private network.

ARS digit conversion examples

The ARS digit conversion table reflects these values:

- ARS feature access code = 9
- AAR feature access code = 8
- Private Network Office Code (also known as Home RNX) = 222
- Prefix 1 is required on all long-distance DDD calls
- Dashes (-) are for readability only

Communication Manager maps the dialed digits to the matching pattern that most closely matches the dialed number.

Example:

If the dialed string is 957-1234 and matching patterns 957-1 and 957-123 are in the table, the match is on pattern 957-123.

ARS digit conversion examples table:

Operation	Actual Digits Dialed	Matching Pattern	Replacement String	Modified Address	Notes
DDD call to ETN	9-1-303-538-1 345	1-303-538	362	362-1345	Call routes via AAR for RNX 362
Long-distance call to specified carrier	9-10222+DDD	10222	(blank)	(blank)	Call routes as dialed with DDD # over private network
Terminating a local DDD call to an internal station	9-1-201-957-5 567 or 9-957-5567	1-201-957-5 or 957-5	222-5	222-5567	Call goes to home RNX 222, ext. 5567
Unauthorized call to	9-1-212-976-1 616	1-XXX-976	#	(blank)	“#” means end of

Operation	Actual Digits Dialed	Matching Pattern	Replacement String	Modified Address	Notes
intercept treatment					dialing. ARS ignores digits dialed after 976. User gets intercept treatment.
International calls to an attendant	9-011-91-67 25 30	011-91	222-0111#	222-0111	Call routes to local server (RNX 222), then to attendant (222-0111).
International call to announcement (This method can also be used to block unauthorized IDDD calls)	9-011-91-67 25 30	011-91	222-1234#	222.1234-	Call routes to local server (RNX 222), then to announcement extension (222-1234).
International call from certain European countries needing dial tone detection	0-00-XXXXXX XX	00	+00+	00+XXXX	The first 0 denotes ARS, the second pair of 0s denotes an international call, the pluses denote “wait” for dial tone detection.

Defining operator assisted calls

About this task

Here is an example of how Communication Manager routes an ARS call that begins with 0 and requires operator assistance. The user dials 9 to access ARS, then a 0, then the rest of the number.

Procedure

1. Type `display ars analysis 0`.

2. Press **Enter** to view the AAR and ARS Digit Analysis Table screen starting with 0.

   We will use the ARS digit analysis table shown above and follow the routing for an operator assisted a call to NJ.

   We will use the ARS digit analysis table shown above and follow the routing for an operator assisted a call to NJ.

   - A user dials 9 0 908 956 1234.
   - Communication Manager drops the ARS FAC (9 in our example), looks at the ARS Digit Analysis Table for 0, and analyzes the number. Then it:

     determines that more than 1 digit was dialed

     rules out the plan for 00, 01, and 011

     determines that 11 digits were dialed
   - Communication Manager routes the call to route pattern 1 as an operator assisted call.

Defining Inter-exchange carrier calls

About this task

Here is an example of how Communication Manager routes an ARS call to an inter-exchange (long-distance) carrier (IXC). IXC numbers directly access your long-distance carrier lines. IXC numbers begin with 1010, followed by three digits, plus the number as it is normally dialed including 0, 00, or 1+ 10 digits. These numbers are set up on your default translations. Remember, the user dials 9 to access ARS, then the rest of the number.

Procedure

1. Type `display ars analysis 1`.
2. Press **Enter** to view the ARS Digit Analysis Table screen starting with 1.

   This table shows five translations for IXC calls.

   When you use `x` in the **Dialed String** field, Communication Manager recognizes `x` as a wildcard. The `x` represents any digit, 0 - 9. If I dial 1010, the next 3 digits will always match the x wild cards in the dialed string.

   Use the ARS digit analysis table shown above and follow the routing for an IXC call to AT&T. 1010288 is the carrier access code for AT&T.

   - A user dials 9 1010288 plus a public network number.
   - Communication Manager drops the ARS FAC (9 in our example), looks at the ARS Digit Analysis Table for 1010, and analyzes the number.

- Then it matches 288 with xxx and sends the call over route pattern 5.

Restricting area codes and prefixes

About this task

Certain area code numbers are set aside in the North American Numbering Plan. These numbers are 200, 300, 400, 500, 600, 700, 800, 877, 888, 900. You need to specifically deny calls made to area codes 200 through 900 (except 800 and 888).

You can also deny access to the 976 prefix, which is set aside in each area code for pay-per call services, if you do not want to incur charges. You can block 976 or any other prefix in all NPAs with a single entry in the digit analysis table. See *Using wild cards* for more information.

Procedure

1. Set the 200 area code apart from other area codes 201 through 209.

   We use the digit analysis table 120 because it defines long distance calls that begin with 1 and all area codes from 200 through 209.

2. To deny long distance calls to the 200 area code, type `change ars analysis 120`.

3. Press **Enter** to view the ARS Digit Analysis Table screen beginning with 120.

   The table (on the screen) in this example shows two translations for calls that begin with 120.

   First, follow the routing for a long-distance call that begins with 120 and is allowed. The 120 translation handles all dial strings 1-201 through 1-209, and there are many matches.

   - A user dials 9 120 plus 8 digits (the first of the 8 digits is not 0).
   - Communication Manager drops the ARS FAC (9 in our example), looks at the **ARS Digit Analysis Table** for 120, and analyzes the number. It determines the call is long-distance and sends the call over route pattern 4

   Now we will follow a call that begins with the restricted area code 200. Only one string matches this translation.

   - A user dials 9 1200 plus 7 digits.
   - Communication Manager drops the ARS FAC (9), and looks at the **ARS Digit Analysis Table** for 1200. It determines that the call type is deny, and the call does not go through.

Using wild cards

About this task

You can use wild cards to help separate out calls to certain numbers. Remember, when you use the wild card `x` in the **Dialed String** field, Communication Manager recognizes `x` as any digit, 0 - 9. For example, you can restrict users from making calls to a 555 information operator where you might incur charges.

Procedure

1. Type `change ars analysis 1`.
2. Press **Enter**.
   The ARS Digit Analysis Table screen beginning with 1 appears.
3. Use the arrow keys to move to a blank **Dialed String** field.
4. Enter `1xxx555` in the **Dialed String** field.
5. Enter `11` in the **Total Min** and `11` in **Total Max** fields.
6. Enter `deny` (denied) in the **Route Pattern** field.
7. Enter `fnhp` in the **Call Type** field.
8. Press **Enter** to save your changes.

Defining local information calls

About this task

You can set up Communication Manager to allow calls to local information, or in this example, 411.

To allow 411 service calls:

Procedure

1. Type `change ars analysis 4`.
2. Press **Enter**.
   The ARS Digit Analysis Table screen beginning with 4 appears.
3. Use the arrow keys to move to a blank **Dialed String** field.
4. Enter `411` in the **Dialed String** field.
5. Enter `3` in the **Total Min** and `3` in **Total Max** fields.
6. Enter `1` in the **Route Pattern** field.

7. Enter `svcl` (service call) in the **Call Type** field.
8. Press **Enter** to save your changes.

Administering Call Type Digit Analysis

Before you begin

There must be at least one entry in the **Call Type Digit Analysis Table** for Call Type Digit Analysis to take place.

Procedure

1. Enter `change calltype analysis`.
   The **Call Type Digit Analysis Table** appears.
2. In the **Match** field, enter the digits the system uses to match to the dialed string.

   The dialed string contains the digits that Communication Manager analyzes to determine how to process the call.

   For example, enter `303` to match any dialed number beginning with 303.
3. In the **length: Min Max** fields, enter the minimum and maximum number of dialed digits for the system to match.
4. Enter up to four digit manipulations for this **Match** string.
5. Enter the number of digits to delete, the number of digits to insert, and the call type against which to test the modified digit string.

Call Type Digit Analysis Example

In our example, this is the administered **Call Type Digit Analysis Table**.

In our example, Communication Manager analyzes 3035554927 for routing.

1. Communication Manager deletes 0 digits, inserts nothing, and searches the resulting 3035554927 against the ARS tables.
2. If there are no matching entries, Communication Manager deletes 0 digits, inserts the digit `1`, and searches the resulting 13035554927 against the ARS tables.

3. If there are no matching entries, Communication Manager deletes 3 digits, inserts nothing, and searches the resulting 5554927 against numbers of **ext** type in the dial plan.
4. If there are no matching entries, Communication Manager deletes 0 digits, inserts `011`, and searches the resulting 0113035554927 against the ARS tables.

Setting up Multiple Locations

Before you begin

Ensure that the **Multiple Locations** field on the System Parameters Customer-Options (Optional Features) screen is set to y. If this field is set ton, contact your Avaya representative for more information. If you are setting up locations across international borders, you must ensure that the **Multinational Locations** field on the System Parameters Customer-Options (Optional Features) screen is also set to y.

Be sure your daylight savings rules are administered. Daylight Savings Rule numbers are located on the Daylight Savings Rules screen.

Each cabinet in a server or switch and each port network in the cabinet must be assigned a location number. See the `add-cabinet` and `change-cabinet` in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

About this task

You can define a location number for:

- Remote Offices
- Media gateways
- IP network regions, used by IP stations and IP trunks

You can create numbering plans and time zone and daylight savings plans that are specific for each location. Choose your main location, and offset the local time for each location relative to the system clock time. The main location is typically set to have offset 0.

For example, we will set up multiple locations for Communication Manager server with cabinets in Chicago and New York. Location 1 is assigned to the cabinet in Chicago, our main office, so Central Standard Time is used for our main location. Location 2 is assigned to the cabinet in New York. We'll define the numbering plan area (NPA) for the Chicago and New York locations, and set the time zone offset for NY to show the difference in time between Eastern Standard Time and Central Standard Time.

Tip:

Type `list cabinets` to see the Cabinet screen and a list of cabinets and their locations.

To define locations for cabinets in Chicago and New York:

Procedure

1. Type `change locations`.
2. Press `Enter`.
   The Locations screen appears.
3. Type `y` in the **ARS Prefix 1 required for 10-digit NANP calls** field.

   Our dial plan requires users to dial a `1` before all 10-digit (long distance) NANP calls.
4. Type `Chicago` in the **Name** field in the **Number 1 row**.

   Use this field to identify the location.
5. Type `+00:00` in the **TimeZone Offset** field in the **Number 1 row**.

   In our example, the system time and the Chicago location time are the same.
6. Type `1` in the **Daylight Savings Rule** field in the **Number 1 row**.

   In our example, daylight savings rule 1 applies to U.S. daylight savings time.

   Tip:

   Use the `display daylight-savings-rules` command to see what rules have been administered on Communication Manager.
7. Type `312` in the **Number Plan Area Code** field in the **Number 1 row**.

   In our example, 312 is the local area code for Chicago, location 1.
8. Type `New York` in the **Name** field in the **Number 2 row**
9. Type `-01:00` in the **TimeZone Offset** field in the **Number 2 row**.

   In our example, subtract one hour from the system clock in Chicago to provide the correct time for the location in New York.
10. Type `1` in the **Daylight Savings Rule** field in the **Number 2 row**.

    In our example, daylight savings rule 1 applies to U.S. daylight savings time, and both locations use the same rule.
11. Type `212` in the **NANP** field in the **Number 2 row**.

    In our example, 212 is the local area code for New York, location 2.
12. Press **Enter** to save your changes.

    See *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information on the Multiple Locations feature.

Routing with multiple locations

Before you begin

Be sure the **Multiple Locations** field on the System Parameters Customer-Options (Optional Features) screen is set to y. If this field is set to n, contact your Avaya representative for more information.

AAR or ARS must be administered.

- For AAR, verify that either the **Private Networking** field or the **Uniform Dialing Plan** field is y on the System Parameters Customer-Options (Optional Features) screen.
- For ARS, verify that the **ARS** field is y on the System-Parameters Customer-Options (Optional Features) screen.

You can define a location number for:

- Remote Offices
- Media gateways
- IP network regions, used by IP stations and IP trunks

About this task

When you set up multiple locations, you can define call routing that covers all locations as well as call routing specific to each individual location. Use your routing tables to define local routing for 911, service operators, local operator access, and all local calls for each location. Leave long-distance and international numbers that apply across all locations on the routing tables with **Location** field set to all.

For example, we will use ARS to set up local call routing for two Communication Manager server locations. Our Chicago server is assigned to location 1, and our New York server is assigned to location 2.

Our example shows a simple local dialing plan. Each location already contains location-specific routing tables. We'll use route pattern 1 for local service calls and route pattern 2 for local HNPA calls in the Chicago location.

Tip:

Create location-specific routing by assigning different route patterns for each location

To define local calls for servers in Chicago and New York:

Procedure

1. Type `change ars analysis location 1`.
2. Press **Enter**.
   The ARS Digit Analysis Table screen for location 1 appears.

3. Type the information for local dialed strings and service calls in each row on the screen.

   In our example, for location 1 (Chicago) local HNPA calls:

   a. Type the appropriate digit in the **Dialed String** field.
   b. Type `7` in the **Total Min** field.
   c. Type `7` in the **Total Max** field.
   d. Type `2` in the **Route Pattern** field.
   e. Type `hnpa` in the **Call Type** field.

   In our example, for location 1 (Chicago) local service calls:

   a. Type the appropriate digits in the **Dialed String** field.
   b. Type `3` in the **Total Min** field.
   c. Type `3` in the **Total Max** field.
   d. Type `1` in the **Route Pattern** field.
   e. Type `svcl` in the **Call Type** field.

4. Press **Enter** to save your changes.
5. Type `change ars analysis 4 location 2`.
6. Press **Enter**.
   The **ARS Digit Analysis Table** for location 2 appears
7. Type in the local HNPA and service call routing information for New York.
8. Press **Enter** to save your changes.

   See Automatic Routing in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information on ARS.

   See Multiple Locations in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205 for more information on the Multiple Locations feature.

Call routing modification

If your system uses ARS Digit Analysis to analyze dialed strings and select the best route for a call, you must change the digit analysis table to modify call routing. For example, you'll need to update this table to add new area codes or to restrict users from calling specific areas or countries.

Adding a new area code or prefix

Before you begin

A common task for system administrators is to configure their system to recognize new area codes or prefixes.

When you want to add a new area code or prefix, you look up the settings for the old area code or prefix and enter the same information for the new one.

Tip:

Use **display toll xxx**, where xxx is the prefix you want to add, to see if the new area code or prefix number is set up as a toll call (y) or not. Some users might not be allowed to dial toll call numbers.

About this task

We will add a new area code. When the California area code, 415, splits and portions change to 650, you will need to add this new area code to your system.

Tip:

If you do not need to use `1` for area code calls, omit the `1` in steps 1, 4, and 7 in our example. Also, enter `10` in the **Total Min** and **Total Max** fields (instead of 11) in step 8.

Procedure

1. Type `list ars route-chosen 14152223333`.
2. Press **Enter**.

   You can use any 7-digit number after 1 and the old area code (415). We used `222-3333`.

   The ARS Route Chosen Report screen appears.
3. Write down the **Total Min**, **Total Max**, **Route Pattern**, and **Call Type** values from this screen.

   In this example, the **Total Min** is **11**, **Total Max** is **11**, **Route Pattern** is **30**, and the **Call Type** is **fnpa**.
4. Type `change ars analysis 1650`.
5. Press **Enter**.
   The ARS Digit Analysis Table screen appears.
6. Move to a blank **Dialed String** field.

   If the dialed string is already defined in your system, the cursor appears in the appropriate **Dialed String** field, where you can make changes.
7. Enter `1650` in the **Dialed String** field.

8. Enter the **minimum** and **maximum** values from step 2 in the **Total Mn** and **Total Mx** fields.
   In our example, enter `11` in each field.
9. Enter the `route pattern` from step 2 in the **Route Pattern** field.
   In our example, enter `30`
10. Enter `fnpa` in the **Call Type** field.
11. Enter the node number from step 2 in the **Node Num** field.
    For our example, leave the node number blank.
12. Press **ENTER** to save your changes.

    To add a new prefix, follow the same directions, except use a shorter dial string (such as list ars route-chosen 2223333, where 222 is the old prefix) and a dial type of `hnpa`.

    Tip:

    If you change an existing area code for a network with multiple locations, be sure to change the **Number Plan Area Code** field on the Locations screen.

Using ARS to restrict outgoing calls

About this task

ARS allows you to block outgoing calls to specific dialed strings. For example, you can restrict users from making international calls to countries where you do not do business, or in the U.S. you can restrict access to 900 and 976 pay-per-call numbers.

Security alert:

To prevent toll fraud, deny calls to countries where you do not do business. The following countries are currently concerns for fraudulent calling.

country	code	country	code
Colombia	57	Pakistan	92
Ivory Coast	225	Peru	51
Mali	23	Senegal	221
Nigeria	234	Yemen	967

To prevent callers from placing calls to Colombia (57):

Procedure

1. Type `change ars analysis 01157`.

2. Press **Enter**.
   a. Enter `011` (international access)
   b. Enter the `country code (57)`

   The ARS Digit Analysis Table screen appears.
3. Move to a blank **Dialed String** field.

   Skip to Step 6 to deny calls to this dialed string

   If the dialed string is already defined in your system, the cursor appears in the appropriate **Dialed String** field.
4. Enter `01157` in the **Dialed String** field.
5. Enter `10` in the **Total Min** and `23` in **Total Max** fields.
6. Enter `deny` (denied) in the **Route Pattern** field.
7. Enter `intl` in the **Call Type** field.
8. Press **Enter** to save your changes.

Overriding call restrictions

Before you begin

Verify that the **Authorization Codes** field on the System Parameters Customer-Options (Optional Features) screen is set to y.

Security alert:

You should make authorization codes as long as possible to increase the level of security. You can set the length of authorization codes on the Feature-Related System Parameters screen.

About this task

You can use authorization codes to enable callers to override a station's calling privileges. For example, you can give a supervisor an authorization code so they can make calls from a telephone that is usually restricted for these calls. Since each authorization code has its own COR, the system uses the COR assigned to the authorization code (and FRL assigned to the COR) to override the privileges associated with the employee's telephone.

Note that authorization codes do not override dialed strings that are denied. For example, if your ARS tables restrict users from placing calls to Colombia, a caller cannot override the restriction with an authorization code.

We will create an authorization code 4395721with a COR of 2.

Procedure

1. Type `change authorization-code 4395721`.
2. Press **Enter**.
   The Authorization Code - COR Mapping screen appears.
3. In the **AC** field, type `4395721`.
4. In the **COR** field, enter `2`.
5. Press **Enter** to save your changes.

ARS Partitions

Most companies want all their users to be able to make the same calls and follow the same route patterns. However, you might find it helpful to provide special calling permissions or restrictions to a group of users or to particular telephones.

ARS partitioning allows you to provide different call routing for a group of users or for specific telephones.

Note:

If you used partitioning on a prior release of Avaya Communication Manager and you want to continue to use partitioning, please read this section carefully. In this release of Avaya Communication Manager, partition groups are defined on the **Partition Route Table**. If you want to define routing based on partition groups, use the **Partition Route Table**. Partition groups are no longer defined on the Digit Analysis Table.

Related topics:

Setting up Time of Day Routing on page 314

Setting up partition groups

Before you begin

- Ensure that the **Tenant Partitioning** field on the System Parameters Customer-Options (Optional Features) screen is `y`.
- Ensure that the **Time of Day Routing** field on the System Parameters Customer-Options (Optional Features) screen is `n`.

About this task

Let us say you allow your employees to make local, long distance, and emergency calls. However, you have a lobby telephone for visitors and you want to allow users to make only local, toll-free, and emergency calls from this telephone.

To restrict the lobby telephone, you modify the routing for a partition group to enable only specific calls, such as U.S. based toll-free 1-800 calls, and then assign this partition group to the lobby telephone.

To enable 1-800 calls for partition group 2:

Procedure

1. Type `list ars route-chosen 18002221000`.
2. Press **Enter**.

   You can use any 7-digit number following the 1800 to create an example of the dialed string.

   The ARS Route Chosen Report screen for `partition group 1` appears.
3. Record the route pattern for the selected dialed string.
   In our example, the route pattern for 1800 is p1. This indicates that the system uses the Partition Routing Table to determine which route pattern to use for each partition.

   > **Note:**
   >
   > If there was a number (with no p) under Route Pattern on the Route Chosen Report, then all partitions use the same route pattern. You need to use the Partition Routing Table only if you want to use different route patterns for different partition groups.
4. Press **Cancel** to return to the command prompt.
5. Type `change partition-route-table index 1`.
6. Press **Enter**.
   The Partition Routing Table screen appears. In our example, partition group 1 can make 1800 calls and these calls use route pattern 30.
7. In the **PGN2** column that corresponds to Route Index 1, type `30`.
8. Press **Enter**.
   This tells the system to use route pattern 30 for partition group 2 and allow partition group 2 members to make calls to 1800 numbers.

Assigning a telephone to a partition group

Before you begin

To assign an extension to a partition group, first assign the partition group to a COR, and then assign that COR to the extension.

Procedure

1. Type`list cor`.
2. Press **Enter**.
3. The Class of Restriction Information screen appears.
4. Choose a COR that has not been used.
   In our example, select 3
5. Type `change cor 3`.
6. Press **Enter**.
   The Class of Restriction screen appears.
7. Type a name for this COR in the **COR Description** field.
   In our example, type **lobby**
8. Enter `2` in the **Partitioned Group Number** field.
9. Now to assign `COR 3` to the lobby telephone at extension 1234:
   a. Type `change station 1234`.
   b. Press **Enter**.
   The Station screen for 1234 appears.
   c. In the **COR** field, enter `3`.
   d. Press **Enter** to save your changes.

Setting up Time of Day Routing

Before you begin

AAR or ARS must be administered on Communication Manager before you use Time of Day Routing.

- For AAR, verify that either the **Private Networking** field or the **Uniform Dialing Plan** field is`y` on the System Parameters Customer-Options (Optional Features) screen.
- For ARS, verify that the **ARS** field is `y` and the **Time of Day Routing** field is `y` on the System Parameters Customer-Options (Optional Features) screen.

About this task

Time of Day Routing lets you redirect calls to coverage paths according to the time of day and day of the week. You need to define the coverage paths you want to use before you define the time of day coverage plan.

You can route calls based on the least expensive route according to the time of day and day of the week the call is made. You can also deny outgoing long-distance calls after business hours to help prevent toll fraud. Time of Day Routing applies to all AAR or ARS outgoing calls and trunks used for call forwarding to external numbers.

As an example, we will allow our executives to make long distance calls during business hours. Let us look at the Time of Day Routing Plan before we make any changes

To display your Time of Day Routing Plan:

Procedure

1. Type `display time-of-day 1`.
2. Press **Enter**.
   The Time Of Day Routing Plan screen for plan 1 appears.

   > ✱ **Note:**
   >
   > Make a note of the routing plan that is currently in effect. In our example, this plan is for employees who can only make local calls.
   >
   > You can see that in our example, two partition group numbers control time of day routing. PGN 1 begins one minute after midnight (00:01) every day of the week, and is used for after-business hours and all day Saturday and Sunday. PGN 2 is assigned to office hours Monday through Friday, not including noon (12:00) to 1:00 p.m. (13:00).

3. Press **Cancel** to clear the screen.

Creating a New Time of Day Routing Plan

Procedure

1. Type `change time-of-day 2`.
2. Press **Enter**.
3. Type `1` in each field as shown on **Time of Day Routing Plan 1**.
   In our example, this is the PGN used for after hours and the lunch hour.
4. Type `3` in all other fields.

In our example, PGN 3 uses the route pattern for long-distance calls during business hours. We can save money by using the trunk lines provided by our new long-distance carrier.

5. Press **Enter** to save your changes.
6. Now assign your new Time of Day Routing Plan 2 to the COR assigned to your executives

   See *Class of Restriction* to view where to assign this field.

   For this example, assume the following:

   - Jim is the user at extension 1234.
   - Extension 1234 is assigned a COR of 2.
   - COR 2 is assigned a Time of Day Plan Number of 1.
   - The Time of Day Routing Plan 1 is administered as shown in the example above.

   When Jim comes into work on Monday morning at 8:30 and makes an ARS call (dials the ARS access code followed by the number of the person he is calling), the system checks the Time of Day Plan Number assigned to Jim’s COR

   Because Jim has a COR of 2 with Time of Day Plan Number 1, the system uses Time of Day Routing Plan 1 to route the call.

   According to Time of Day Routing Plan 1, calls made between 8:00 a.m. and 11:59 a.m. route according to the route pattern set up on PGN 1.

   If Jim makes a call between 12:00 p.m. and 1:00 p.m. on Monday, the Time of Day Routing Plan 1 is used again. However, this time the call is routed according to PGN 2.

Setting up a Remote user by Network region and Time zone

About this task

With your system located in New York and a remote user located in Germany, to create the correct time zone settings:

Procedure

1. Type `change locations`.
2. Press `Enter`.

   The Locations screen displays.

3. In the **Name** field, enter the name of the location (for instance, Germany).
4. In the first **Timezone Offset** field, enter `+` to indicate the time is ahead of the system time.
5. In the second **Timezone Offset** field, enter `08` for the number of hours difference between this location and system time.
6. In the **Daylight Savings** field, enter `1` if this country has daylight savings.
7. Press `Enter` to save your changes.
8. Type `change ip-network-map`.
9. Press `Enter`.
   The IP Address Mapping screen displays.
10. In the **From IP Address** field, enter the IP address for the remote station in Germany.
11. In the **To IP Address** field, enter the IP address of your system.
12. In the **Subnet** or **Mask** field, enter the subnet mask value of your network
13. In the **Region** field, enter a number that is not being used. In this example, enter `3`.
14. Press `Enter` to save your changes.
15. Type `change ip-network-region 3`.
16. Press **Enter**.
    The IP Network Region screen displays.
17. In the **Name** field, enter the location name for familiarity.
18. In the **Location** field, enter the number from the Locations screen. In this example, it was `11`.
19. Press **Next Page** until you get to page 3, the Inter Network Region Connection Management screen.
20. Notice in the **src rgn** column that a 3 displays, and under **dst rgn** a 1, indicating that Network Region 3 (Germany) is connected to Network Region 1 (New York) using Codec Set 1.
21. Press `Enter` to save your changes

    See *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information on the Multiple Locations feature.

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.

Setting up no-cadence call classification modes

About this task

Procedure

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

About this task

Procedure

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.

Alerting Tone for Outgoing Trunk Calls

Use the Alerting Tone for Outgoing Trunk Calls feature to apply an alerting tone to an outgoing trunk call after an administrable amount of time.

Setting the outgoing trunk alerting timer

Procedure

1. Enter `change cor n`, where *n* is the number of a specific COR.
2. Click **Next** until you see the **Outgoing Trunk Alerting Timer (minutes)** field.
3. In the **Outgoing Trunk Alerting Timer (minutes)** field, specify when the initial alerting tone must be applied to the call.
4. Select **Enter** to save your changes.

Setting the trunk alerting tone interval

Procedure

1. Enter `change system-parameters features`.
2. Click **Next** until you see the **Trunk Alerting Tone Interval (seconds)** field.
3. In the **Trunk Alerting Tone Interval (seconds)** field, specify the interval at which the alerting tone must be repeated on the call.
4. Select **Enter** to save your changes.

Chapter 12: Multimedia Calling — Multimedia Applications Server Interface

The Multimedia Applications Server Interface (MASI) defines a protocol and a set of operations that are used to extend Avaya Communication Manager feature functionality to a Multimedia Communications Exchange (MMCX) system. MASI architecture fits the client/server model, where Avaya Communication Manager functions as a server for MMCX clients. Examples of features supported by MASI include call detail recording (CDR), Communication Manager Messaging, and Automatic Alternate Routing (AAR)/ Automatic Route Selection (ARS).

MMCX can make use of both MASI features and MMCX autonomous features. Autonomous features are those that MMCX provides, even if MASI is not enabled. This document does not discuss them unless there is a consideration for MASI administration.

Some autonomous MMCX features:

- Basic Call (Place/Drop)
- Call Coverage
- Conference
- Transfer

Avaya Communication Manager /MASI features:

- Basic Call (Place/Drop) - Avaya Communication Manager tracks the status of all calls placed to or from a MASI terminal.
- Call Detail Recording - Avaya Communication Managertracks calls to and from MASI terminals and can produce call records that indicate if a call uses MASI
- Call Coverage - Avaya Communication Manager tracks MMCX calls that are sent to coverage. A Communication Manager coverage path can contain both MASI terminals and Communication Manager stations.
- Conference - Avaya Communication Manager tracks conference calls that involve MASI terminals, if a Communication Managerstation originates the conference. Conferences that involve MASI terminals and Communication Manager stations are voice-only. If the Communication Manager station originates the call, the caller can use the consultative form of conference or transfer.
- World Class Routing (AAR or ARS) - Calls from MASI terminals can take advantage of Avaya Communication Manager World Class Routing capabilities.
- Voice messaging access to AUDIX/INTUITY - MMCX users can take advantage of AUDIX voice messaging, and receive message waiting indication.
- MMCX trunking - By assigning trunk access codes to interfaces from the MMCX to other MMCXs or the PSTN, Avaya Communication Manager can monitor traffic over those interfaces.

Prerequisites— Multimedia Applications Server Interface

For purposes of administration, there are feature buttons and groups of users that you must not administer with MASI terminal extensions. There are also features that you simply cannot administer for a MASI terminal, because the software does not allow it.

⚠ **Caution:**

Avaya Communication Manager offers a wide range of features, and MMCX users might want to take advantage of this. In some cases, these features will operate as expected. However, some features are not supported for use over the MASI link, and their behavior is unpredictable. You might cause harm to your system by attempting to use these features. The Interactions section contains a list of features, and lists those features that are absolutely not supported for use with MASI. If you administer features on the DO NOT ADMINISTER list, Avaya cannot be responsible for the result.

Before you start to administer MASI, you should make a plan for how to do it. Among the configurations on the following pages, there is probably one that matches the configuration of your system fairly closely. You might want to either write on these pages, or draw up your own configuration. It might help you if you have already determined trunk group and signaling group numbers, unused extensions, and so on. The following are things you need to consider:

- Establish the dial plan on the MMCX to agree with that of Avaya Communication Manager. If you use Universal Dial Plan and MMCX, you might need to make adjustments for the MMCX dial plan.
- Find unused extensions and trunk group numbers. You need:
- one trunk group number for each ISDN-PRI connection to the MMCX
- one signaling group number for each MASI node and an unused Communication Manager extension for the signaling group
- one unused Communication Manager extension for the Near-End Path Termination number for all MASI Paths to this ECS. You can use the same number for all MASI nodes in the domain
- two unused MMCX extensions for the nearpath and tscnum arguments to the chgmasi command. This is the command you use to administer MASI on the MMCX.

List of terms

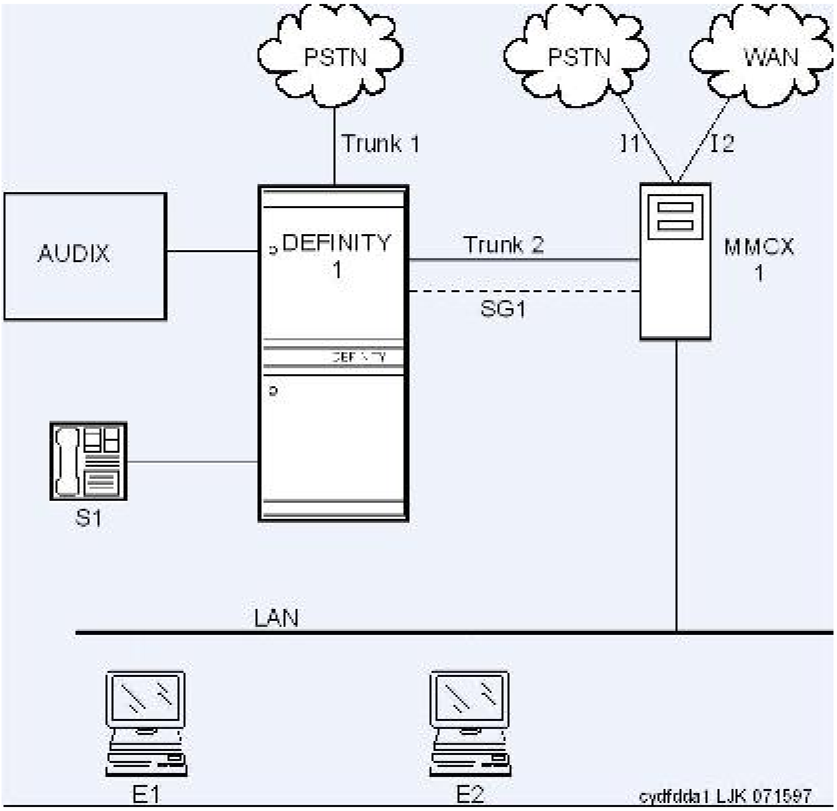
This is a list of terms that are specific to MASI, or that have meanings in the context of MASI that are not standard.

- chgmasi - The command you use to administer MASI at the MMCX administration terminal.
- Interserver - Connections between MMCX terminals on different MMCX servers/nodes.
- MASI domain - A MASI domain consists of Communication Manager and one or more MASI nodes that share the same dial plan. That is, the extension numbers on the MMCX are known to Communication Manager, and fit in the Communication Manager dial plan.
- MASI interworking - MASI interworking refers to the completion of a voice connection within Communication Manager, involving at least one MASI terminal and a MASI path.
- MASI link - The connection between the MMCX and Communication Manager.
- MASI node - A single MMCX server. You can connect more than one MASI node to a Communication Manager. Each node has a separate number. This node number needs to be consistent whenever referring to a specific MMCX server.
- MASI non-interworking - MASI non-interworking refers to the completion of a call by MMCX, not involving a MASI path.
- MASI path - The Integrated Services Digital Network (ISDN) B-channels between MMCX and Communication Manager in a MASI environment. Paths are used for voice and data connections between Communication Manager and MMCX.
- MASI signaling link - ISDN D-channel used to transport a new ISO protocol called the MASI protocol between Communication Manager and the MMCX.
- MASI terminal - The representation in Communication Manager of MMCX terminals in a MASI environment.
- MMCX interface - PRI interface for connecting an MMCX server to other public, private or wide area network (WAN) switching systems or equipment that is part of the public network. Similar to a Communication Manager trunk group. These can include non-MASI trunks connecting Communication Manager and the MMCX.
- MMCX trunk - The representation in Communication Manager of trunk or network facilities terminating on MMCX. For purposes of MASI, they are called "interfaces."

Configurations— Multimedia Applications Server Interface

There are several ways to set up combinations of MASI nodes and DEFINITY servers.The following figures depict several possible configurations.

Figure 135: MASI domain of Avaya Communication Manager running on one DEFINITY Server and one MMCX



The parts of this drawing, for MASI, are as follows:

- Trunk 1 — This is any type of trunk connection to the public network
- Trunk 2 — This is the link between the Avaya Communication Manager solution and the MMCX, and requires a TN464C or later DS1 circuit pack. You administer this link as an ISDN-PRI trunk group, a MASI path and an NCA-TSC
- I1 and I2 — These are MMCX interfaces to destinations other than Avaya Communication Manager. Administer as MASI trunks
- E1 and E2 — Endpoints (terminals) belonging to the MMCX. Administer as MASI terminals

- MMCX — Determine a node number for each MMCX server. This can be any number from 1 to 15. Once the node number is established, Avaya Communication Manager informs the MMCX of its node number.
- S1 — Avaya Communication Manager station.

Figure 136: MASI domain of Communication Manager running on one DEFINITY Server and two (or more) MMCXs

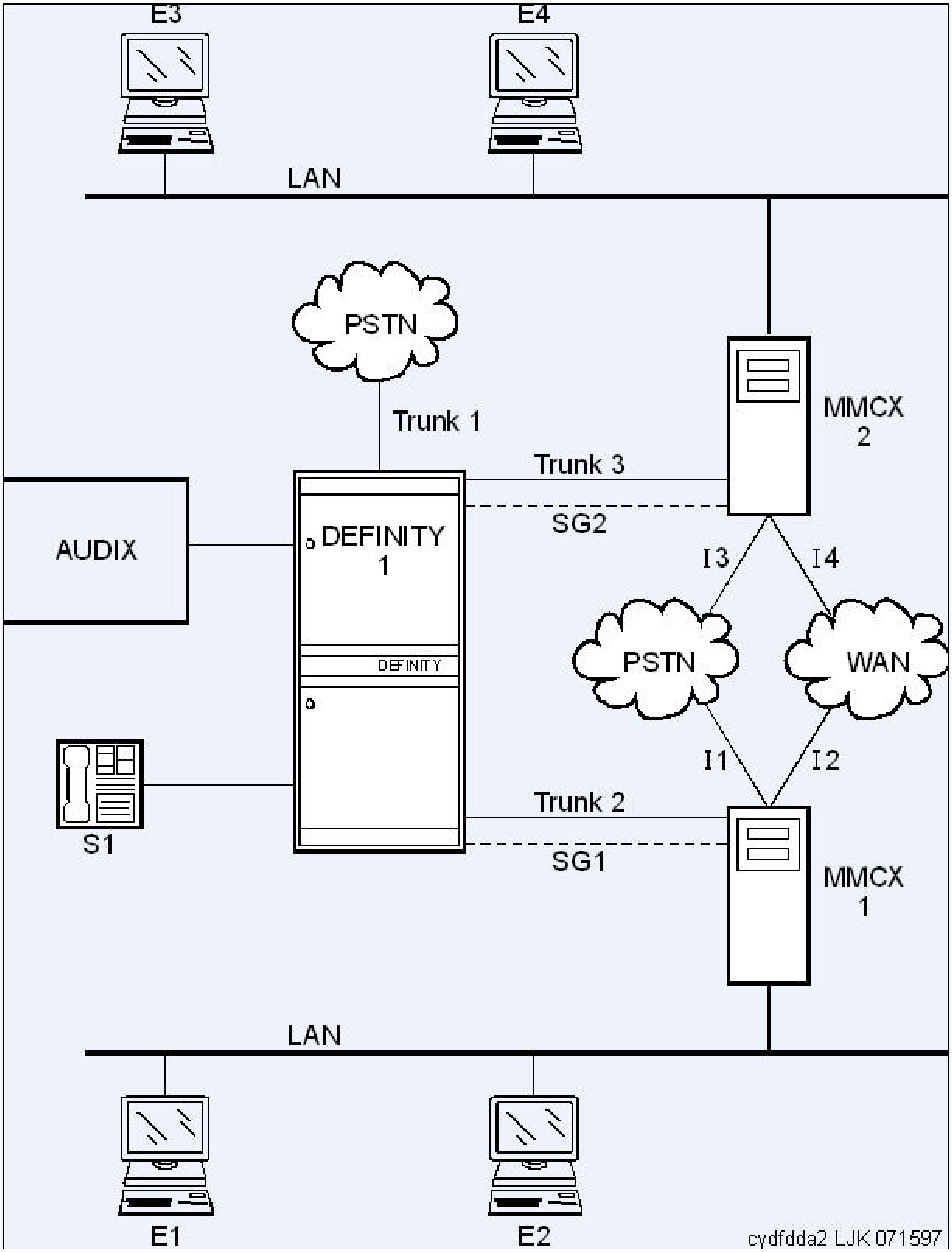


Figure 137: Two separate MASI domains

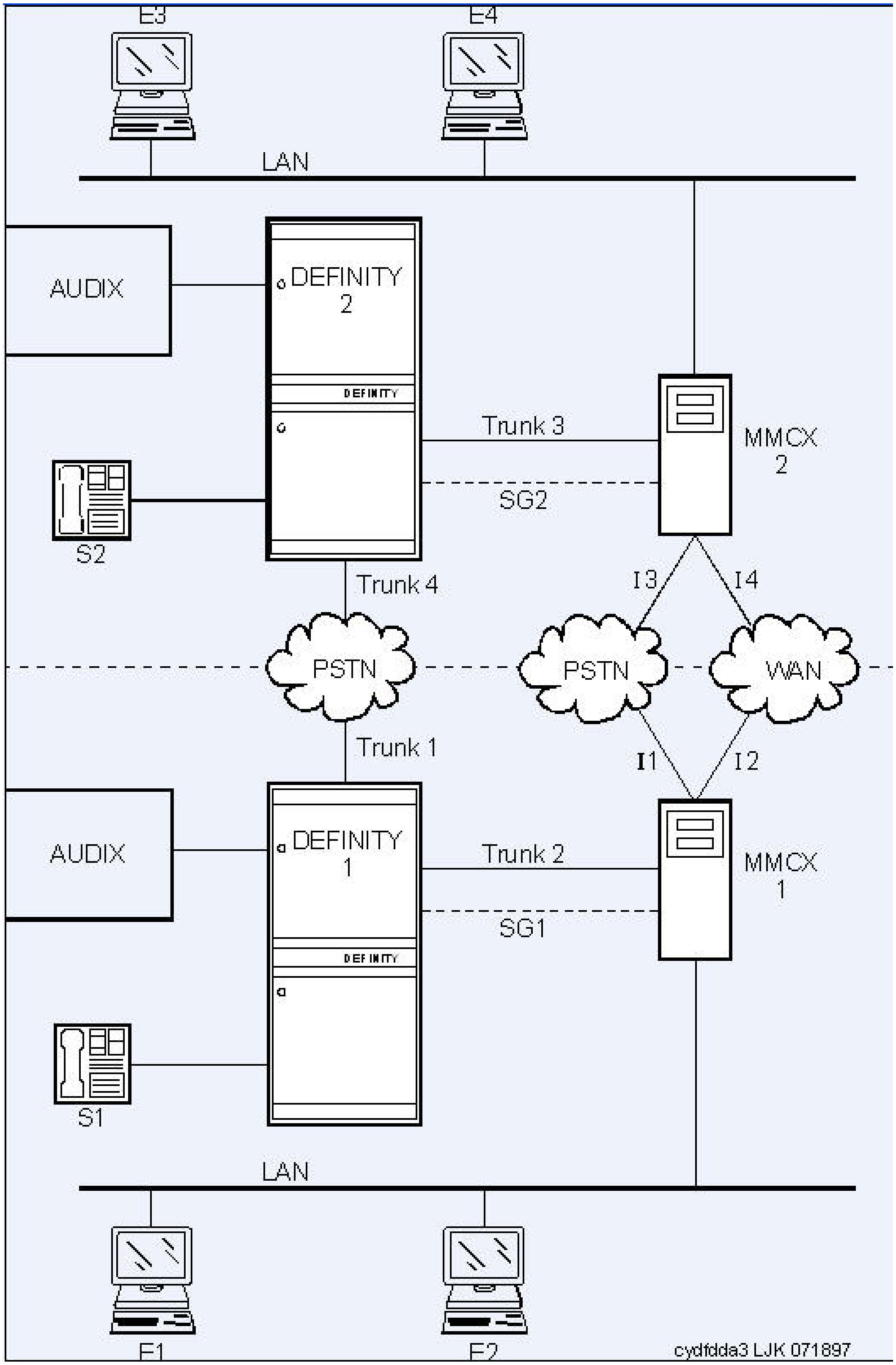
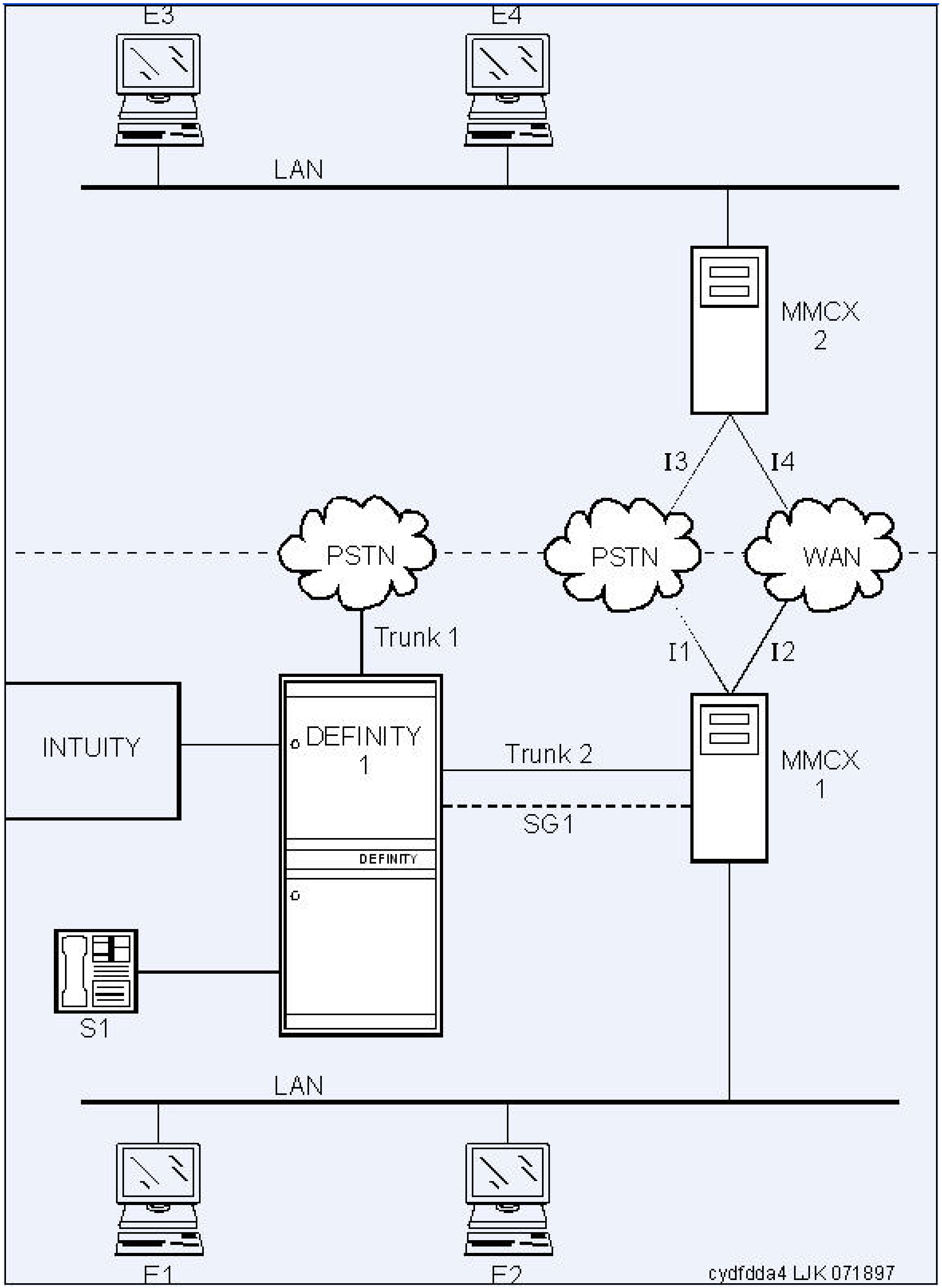


Figure 138: One MASI domain, and one non-MASI MMCX


E3
E4
LAN
MMCX
2
I3
I4
PSTN
PSTN
WAN
Trunk 1
I1
I2
INTUITY
DEFINITY
1
DEFINITY
Trunk 2
SG1
MMCX
1
S1
LAN
E1
E2
cydfdda4 LJK 071897

The MASI node must be directly connected to the Avaya DEFINITY Server for MASI features to work. In this configuration, terminals that belong to MMCX 2 (E3 and E4) do not take advantage of MASI capabilities

Multimedia Applications Server Interface Administration

This section discusses the administration required to make MASI work. You perform most of this administration from the DEFINITY Server administration terminal. However, there are a few things you must do at the MMCX administration terminal. This section sometimes refers to the `chgmasi` command. This is the command you use to administer MASI parameters on the MMCX. For more information about using the `chgmasi` command, see your MMCX documentation.

Related topics:

MASI with Communication Manager features on page 339

Establishing Customer Options

Procedure

On the MMCX, MASI must be enabled using the `chgmasi` command.

An Avaya technical support representative must activate MASI using the System-Parameters Customer-Options (Optional Features) screen. The technical support representative should also verify that ISDN-PRI over PACCON (for DEFINITY Server CSI configurations), and AAR/ ARS are enabled.

Establishing maintenance parameters and alarming options

Procedure

Using the `set options` command (Avaya init or inads logins only), set MASI alarming options.

Note:

Ensure that on the Maintenance-Related System Parameters screen, the **Packet Bus Activated** field is y.

For more information, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300432.

Establishing the physical connection

Procedure

Establishing the physical connection: Establish the physical connection between the Avaya DEFINITY Server and the MMCX.

Administering the Circuit Pack

Procedure

Using the DS1 Circuit Pack screen, verify that the DS1 circuit pack you use to establish the MASI link is administered as follows:

- Bit Rate = 1.544
- Line Coding = b8zs
- Line Compensation = 1
- Signaling Mode = isdn-pri
- Interface = network
- Country Protocol = 1
- Protocol Version = a

Administering the Signaling Group

Procedure

Administering a signaling group: For each MASI node, you need to establish a unique signaling group. Use the command `add signaling-group xxx` to access the Signaling Group screen.

For each link, establish a Non-Call Associated Temporary Signaling Connection (NCA-TSC) with the following attributes:

- **Associated Signaling** - MASI requires **Facility Associated Signaling**, so this field must be set to y.
- **Primary D-channel** - Enter a 6- to 7-character port number associated with the DS1 Interface circuit pack port. The port address of the PRI that carries D-channel signaling.

  The port number is used to assign the primary D-channel in the Signaling Group. For 24-channel facilities, the 24th port is assigned as the D-channel. For 32-channel facilities, the 16th port is assigned as the D-channel.
- **Max Number of NCA TSC** - For MASI, this must be 1.
- **Max number of CA TSC** - Leave the default of 0.
- **Trunk Group For NCA TSC** - This can be left blank
- **Trunk Group for Channel Selection** - This can be left blank
- **Supplemental Service Protocol** - Values are a (AT& T) and b (Qsig).
- **Network Call Transfer?** - Values are y (yes) and n (no).
- **Service/Feature** - Leave blank.
- **As-needed Inactivity Time-out (min)** - This field only applies to as-needed NCA-TSCs. Since MASI requires a permanent connection, leave blank.
- **TSC Index** - This display-only field specifies the administered NCA-TSCs assigned
- **Local Ext** - Enter a valid, unassigned Avaya Communication Manager extension. This extension does not need a port assignment and does not need to correspond to any other administration.
- **Enabled** - Enter `y` to enable the administered NCA-TSC. You might want to wait to enable this link until all other administration is in place. If this is y, Avaya Communication Manager attempts to establish the connection as soon as you submit the form. This might cause your system to alarm, if other administration is not finished
- **Establish** - Used to indicate the strategy for establishing this administered NCA-TSC. Enter `permanent` for MASI.
- **Dest. Digits** - A valid MMCX extension. This must correspond to the value of the tscnum argument to the `chgmasi` command.

  Note:

  These digits are sent as entered to the destination MMCX; no routing or other digit manipulation is performed
- **Appl**. - Specifies the application this administered NCA-TSC is going to be used for. Enter `masi`.

- **Machine ID** - Used to indicate the MASI node to which this administered NCA-TSC is connected. This number should be the same as the MASI node number found on other screens.

Listing or determining status of TSCs To determine which TSCs are designated for MASI, use the`list masi tsc` command.

This command displays the following:

- **Sig Grp** — The number of the signaling group to which this TSC belongs
- **Primary D-Channel** — Port location of the Primary D-channel
- **TSC Index** — The number of the MASI TSC within the signaling group
- **Local Ext**. — Communication Manager extension associated with the TSC
- **Enabled** — Indicates the state of the connection - enabled (y/n)
- **Established** — Value of established flag (as-needed/permanent)
- **Dest. Digits** — The MMCX extension that indicates the TSC destination
- **Mach. ID** — MASI node number

Note:

Once you establish and enable the signaling group, you need to verify that it is active. Use the command `status signaling-group signaling-group#` or `status tsc-administered signaling-group# [/tsc-index] [print]` to determine if the link is active.

Administering ISDN-PRI Trunk Group

Procedure

Use the command `add trunk-group xxx` to access the Trunk Group screen

For a more detailed description of the ISDN-PRI trunk group, see the documentation on *Trunk Group*.

Establish an ISDN-PRI trunk group with the following attributes:

- Group Type = isdn-pri
- TAC = valid TAC that conforms to your existing dial plan
- Direction = two-way
- Service Type = tie
- CDR Reports = n

You must also administer the PRI link from the MMCX to the ECS, using the MMCX administration terminal. See your *MMCX documentation* for information on the `addpri` command.

Administering MASI Path Parameters

Procedure

Use the `change masi path-parameters` command to access the MASI Path Parameters screen.

Establish a MASI Path with the following attributes:

- **Near-End Path Extension** — An unassigned Communication Manager extension. When using the `chgmasi` command to administer the MMCX, this is the farpath extension. See your *MMCX documentation* for more information.
- **MASI Node** — The node number for the MMCX. For each MMCX/MASI node, this number must be the same everywhere it occurs (Signaling Group, MASI Trunk Group, and MASI Terminal screens).
- **Trunk Group** — This is the trunk group number in Communication Manager for the ISDN-PRI trunk that will be used to establish call paths.
- **Far-End Path Termination Number** — This is an unassigned MMCX extension. When using the `chgmasi` command to administer the MMCX, this is the nearpath extension. See your *MMCX documentation* for more information.

Administering MASI Trunk Groups

Procedure

1. Use the MASI Trunk Group screen to define MMCX interfaces that interconnect MASI nodes, or that connect MMCX nodes to another private switch or central office. Examples of MMCX interfaces include:
   - PRI trunks linking MMCX servers
   - PRI trunks linking MMCX to the PSTN
   - PRI trunks from MMCX to Avaya Communication Manager that are used for purposes other than MASI
   - LAN interfaces linking MMCX servers
2. Use the command `add masi trunk-group xxx` (or ‘next’) to access the MASI Trunk Group screen. The trunk group number must not be assigned, and you cannot

exceed the maximum total trunks for your system. Valid values for xxx are unused trunk group numbers in Avaya Communication Manager between 1 to 96 for DEFINITY Server CSI configurations.

- **Group Number** - This field displays the MASI trunk group number. This is the number assigned when executing the `add masi trunk-group` command.
- **CDR Reports** - Valid entries are y, n, and r. Default is y.
    - If you enter y, Call Detail Recording (CDR) records will be generated by completed outgoing calls terminated on this trunk group. If incoming calls are being recorded (the **Record Outgoing Calls Only** field on the CDR System Parameters screen is set to n), then a single CDR record will be generated for answered calls with the call duration.
    - If you enter n, no CDR records will be generated by calls originated by or terminated on this trunk group.
- **Group Name** - Enter a unique name that identifies the trunk group. Up to 27 characters can be used; default is INCOMING CALL.
- **COR** - Enter a Class of Restriction (COR) number (0 to 995) that reflects the desired restriction; default is 1.
- **TN** - This field displays the Tenant Partition number. All MASI trunks are associated with Tenant 1.
- **TAC** - Enter the trunk access code (TAC) that identifies the trunk group on CDR reports. You must assign a different TAC to each MMCX interface. Valid entries conform to the dial plan (1 to 4 digits, * and # are valid first digits).
- **MASI Node Number** — The node number assigned to this MMCX machine.
- **Remote Group Number** — This is the number of the remote trunk group. For ISDN-PRI interfaces, valid values are any number 1 to 8; for local area network (LAN) or WAN calling interfaces, the value must be 9. The combination of MASI Node Number and Remote Group Number must be unique. Remote group number corresponds to the group number on the MASI node.

Viewing a list of all MASI trunk groups

- To view a list of all the MASI trunks administered on the ECS, use the command `list masi trunk-group`.

Determining the status of MASI trunk groups

- To determine the status of a specific MASI trunk, use the command status `masi trunk-group xxx`, where xxx is the trunk group number. This command provides descriptive information about the trunk, and the number of currently active trunk calls.

Related topics:

1-number access on page 373

Administering MASI Terminals

Procedure

Use the `add masi terminal xxxxx` or next command to administer each MASI terminal as a MASI terminal. You use available extensions on the ECS, so they need to conform to the Avaya Communication Manager dial plan. The extension must match the Communication Manager dial plan, and for the add command, the extension must not already be in use. The extension of the MASI terminal must match the number of the MASI terminal. Avaya Communication Manager users dial the MASI Terminal Extension to reach MMCX users

Note:

Anytime you add a terminal or other extension to the MMCX, you must administer a corresponding MASI terminal on Avaya Communication Manager. If you do not, you will not be able to dial this extension from Avaya Communication Manager.

- **Extension** —This field displays the extension that you entered on the command line.
- **BCC** — This field displays the bearer capability class of the terminal, and identifies the type of traffic the terminal supports. For MASI, this is always 0, for voice or voice-grade data.
- **MASI Node Number** — The number of the node on which this terminal resides.
- **TN** — The tenant partition in which this terminal resides. At present, all MASI terminals must reside within tenant 1. This field is display-only, and always 1.
- **COR** — The class of restriction associated with this terminal.
- **Name** —The name associated with the terminal. This can be any alphanumeric string up to 27 characters.
- **Send Display Info** — Indicates whether Avaya Communication Manager should forward display information associated with a call. Set to `y`.
- **LWC Reception** — This field indicates whether the terminal can receive Leave Word Calling (LWC) messages. Valid values are none, audix, and mas-spe (for DEFINITY Server CSI configurations). SPE-based LWC is not supported for MASI terminals. However, if embedded AUDIX is used without a Data Control Link, you must administer MASI terminals to receive SPE-based LWC messages. For such cases, the LWC feature is used by AUDIX messaging systems to activate and deactivate message waiting lamps on MASI terminals.
- **CDR Privacy** – Indicates whether CDR Privacy is supported for this terminal. See Call Detail Recording in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205 for more information.

- **Room** - Enter up to 10 characters to identify the MASI terminal location. This field can be blank.
- **Jack** - Enter up to 5 characters to identify the location where the MASI terminal is connected. This field can be left blank.
- **Cable** - Enter up to 5 characters to identify the cable that connects the MASI terminal to the system. This field can be left blank.
- **Floor** - Enter up to 7 characters to identify the floor where the MASI terminal is located.
- **Building** - Enter up to 7 characters to identify the building where the MASI terminal is located. Valid entries are listed in the site table.
- **BUTTON ASSIGNMENTS** — This field contains a call appearance button and is display only.

Duplicating MASI Terminals

Procedure

Once you have one MASI terminal administered to your liking, you can use the `duplicate masi terminal` command to administer other stations with the same characteristics.

Listing MASI Terminals

Procedure

1. To view a list of all the MASI terminals administered on a server, use the command `list masi terminals`.

   This command only lists terminals within the domain of the Avaya DEFINITY Server from whose SAT you issue the command.
2. To view the active or idle status of a specific MASI terminal, use the command `status masi terminal(extension)`.
3. To determine which extension you assigned as the MASI Near-End Path Termination extension, use the command `list extension-type`.

   This command displays the extension number and type (attendant, masi-terminal, etc.), as well as other information about the extension.

Administering Features

Procedure

1. AAR/ARS: To verify that this feature is enabled, use the command `display system-parameters customer-options`..

   AAR/ARS is an optional feature on Avaya Communication Manager, and you need to purchase this option to use it with MMCX. If it is not enabled, contact your Avaya representative.

   a. The MMCX dial plan must use the same feature access codes as Avaya Communication Manager. If this is not already the case, modify the MMCX dial plan using the `chgdp` command.

      See your MMCX documentation for more information.

   b. Include this feature access code in the `chgmasi` command.

2. CDR: To get call detail records for calls over MMCX interfaces, set CDR Reports =`y` on the MASI Trunk Group screen.

   a. To get call records for calls over the ISDN-PRI trunk group, set CDR Reports = `y` on the ISDN-PRI Trunk Group screen.
   b. To track calls between a MASI terminal and other MASI terminals or Communication Manager stations, enter the MASI terminal extension on the Intra-switch CDR screen.
   c. Enter `n` in the **Record Non-Call Assoc TSC** field on the CDR System Parameters screen.

   Note:

   If you use the same PRI trunks for MASI and non-MASI calls, Avaya strongly recommends that you do not enable CDR for these calls. Establish a separate trunk group for non-MASI calls and set CDR Reports = `n`.

3. Coverage: To establish coverage from a MASI terminal to AUDIX:, use the MMCX user interface to enter the AUDIX hunt group extension as the coverage point. You cannot use Avaya Communication Manager coverage administration for MASI terminals.

   a. If AUDIX ports are not administered in Avaya Communication Manager, you must administer them.
   b. Set up the MASI terminal as an AUDIX subscriber. Enter the MASI terminal extension in the **Extension** field on the Subscriber Administration screen.

4. To establish coverage from a MASI terminal to another MMCX terminal or Avaya Communication Manager station, use the MMCX user interface to enter the desired extension as the coverage point for the MASI terminal.

You cannot use Avaya Communication Manager coverage administration for MASI terminals.

Verifying Administration

About this task

You should make test calls from Avaya Communication Manager to MMCX, to ensure that you can indeed place and receive calls

Procedure

1. Call an unattended MASI terminal.
2. Verify that the call goes to AUDIX..
3. Retrieve the call from the MASI terminal.
4. Verify that all works as expected.

Setting MASI command permissions

About this task

If you are the super-user for your system, you can restrict other administrative logins from changing MASI administration.

Procedure

1. To do this, use the `change permissions(login-ID)` command.
2. Enter `y` in the **Additional Restrictions** field, then move to the Restricted Object List page of the screen.

   You can restrict the following MASI-related objects:

   - masi-path-parameters
   - masi-terminal
   - masi-trunk-group
   - masi-tsc

MASI with Communication Manager features

- AAR/ARS — MMCX can take advantage of advanced routing features for voice-only calls to the public switched telephone network (PSTN) or an Avaya private network. Users must enter the AAR/ ARS access code before the rest of the dialed digits. MASI will route the call over the Communication Manager private network (AAR) or the public network (ARS), based on digits supplied by the MMCX user. Routing patterns must contain only trunk groups that actually terminate to Avaya Communication Manager. Calls from one MMCX to another MMCX do not use AAR/ARS. Authorization codes are not supported.
- Call Detail Recording — Using the MASI link, Avaya Communication Manager is able to track call detail information for calls made using MMCX terminals and interfaces. CDR records all calls originating from or terminating at a MASI terminal. MASI CDR does not record ineffective call attempts when all MASI paths are busy.

  The Resource Flag value of 8 indicates a MASI call. This field appears in unformatted, int-isdn, expanded and customized CDR formats. For formats other than these, you can determine that a call involves a MASI terminal or trunk by the trunk access code (TAC), dialed number or calling number fields. The following are the CDR capabilities of MASI. Administration information is under the heading *How to administer MASI*.

  - Incoming/Outgoing Trunk Call Splitting: Call splitting does not produce separate records for MMCX calls that are transferred or conferenced.
  - intra-switch CDR: You can administer intra-switch CDR to monitor MASI terminals. To do this, simply add the MASI terminal extension on the Intra-switch CDR screen. Avaya Communication Manager then monitors calls from MASI terminals to other MASI terminals, and calls between MASI terminals and Communication Manager stations.
  - CDR Privacy: You can administer a MASI terminal for CDR Privacy.
  - Account Code Dialing and Forced Entry of Account Codes: This is not supported for MASI terminals. Therefore, make sure the COR you assign does not force entry of account codes.
  - Trunk CDR: You can get call detail records for all incoming and outgoing calls made over MMCX interfaces.
- Call redirection / Voice-messaging access — MMCX users can enter an Avaya Communication Manager extension, including an AUDIX hunt group, Callmaster agent, attendant console or telephone as their coverage point. If AUDIX is established as the MASI terminal’s coverage point, the MASI terminal receives message waiting indication, and dials the AUDIX hunt group extension to retrieve messages. Once connected to AUDIX, operation for the MMCX user is the same as for a Communication Manager station user, including use of # to identify the extension, if desired.

  Note:

  It is not possible to determine the call coverage status of a MASI terminal.

Avaya Communication Manager tracks calls to MASI terminals that follow the autonomous coverage path from the MASI terminal. MMCX calls redirected to Communication Manager stations contain display information

MASI terminals that dial AUDIX directly, or that place calls to MASI terminals that cover to AUDIX, do not receive ringback if all AUDIX ports are busy. Instead, these callers see a message the called party is busy, and the call drops.

- Transfer — MASI terminals cannot transfer calls to Communication Manager stations, and cannot transfer a call to another MASI terminal if the call involves a Communication Manager station.
- Conferencing — Conferences can involve both MASI terminals and Avaya Communication Manager stations, and either one can initiate the conference. Communication Manager stations participate in such conferences in voice-only mode. If an MMCX user initiates a conference that involves Communication Manager stations, the conference will drop when the initiator drops from the call. If a Communication Manager station initiates the conference, that station can drop without affecting the other conferees.
- Status tracking - terminals and trunks — Avaya Communication Manager tracks the active/idle status of all MASI terminals, and monitors traffic over MMCX interfaces.
- Trunk groups — For MASI purposes, there are two kinds of trunk groups: the ISDN-PRI trunk groups that serve as paths for establishing calls between Avaya Communication Manager stations or trunks and MASI terminals or interfaces, and the remote trunks that are interfaces from the MMCX to other entities. Each MASI remote trunk group appears to Communication Manager as a single unit, with no concept of members within the group.

Note:

You cannot test, busy out, or release MASI remote trunk groups, since you cannot dial a MASI remote trunk TAC from the Avaya DEFINITY Server. The TAC merely identifies the trunk to Avaya Communication Manager for purposes of status and CDR records.

You cannot administer MASI trunks as part of Communication Manager route patterns.

Related topics:

Multimedia Applications Server Interface Administration on page 329

Unsupported Communication Manager features

We can generalize feature interactions to some extent. For example, since there are no buttons available to a MASI terminal, any feature that requires a button is also not available. MASI cannot support features that require the user to dial a trunk access code for a MASI remote trunk, or a feature access code other than AAR/ARS. The MMCX dial plan can contain only those feature access codes that are supported

⚠ **Caution:**

DO NOT ADMINISTER the following features! The following features are not supported for use over the MASI link, and Avaya cannot be responsible for the results if you attempt to administer them.

Unsupported Call Center features

- ASAI — You must not administer a MASI terminal in an ASAI domain. MASI terminals and MMCX trunks are not monitored by ASAI. It might be possible for a MASI terminal to place a call to a Communication Manager station that is part of an ASAI domain. ASAI will not be blocked from controlling this call, but there can be unpredictable results. The same is true for calls originating from an ASAI domain terminating at MASI terminals, and for ASAI-monitored hunt groups that contain MASI terminals.
- Automatic Call Distribution — You must not include a MASI terminal extension as part of an ACD hunt group. You must not mix MASI administration with anything related to ACD, including Outbound Call Management and PASTE.
- Call Vectoring — You must not include MASI terminal extensions in any step of a vector.

Unsupported Basic features

- Bridged Call Appearances — You must not administer a bridged appearance that involves a MASI terminal
- Call Coverage — You must not administer a MASI terminal in the coverage path of an Avaya Communication Manager station
- Call Forwarding — You must not forward a Communication Manager station to a MASI terminal
- Call Pickup — You must not administer a MASI terminal as part of a pickup group
- Intercom — You must not administer MASI terminals as members of any type of intercom group.
- Manual Message Waiting — You must not administer a manual message waiting button (man-msg-wt) with a MASI terminal as the referenced extension
- Manual Signaling — You must not administer a manual signaling button (signal) with a MASI terminal as the referenced extension.
- Night Service — You must not administer a MASI terminal as a night service destination
- Pull transfer — MASI terminals cannot perform a pull transfer operation. You must not administer this feature on an Avaya DEFINITY Server where MASI is active. This applies only in Italy.
- Station Hunting — You must not administer a MASI terminal as part of a station hunting path.
- Terminating Extension Groups — You must not administer a MASI terminal as part of a TEG.

Constraints with other Communication Manager Fetaures

The following section describes feature behaviors that might not be as expected, but that are not likely to be destructive.

Attendant Features

Features	Constraints
Dial Access to the Attendant	MASI terminals will be able to dial the attendant access code, if it is administered in the MMCX dial plan.
Attendant Direct Extension Selection	Attendants are able to access MASI terminals via DXS buttons and busy lamp indicates status of the MASI terminal.
Emergency Access to the Attendant	MASI terminals have emergency access using the attendant access code, if it is administered in the MMCX dial plan. However, off-hook alerting is not administrable.
Attendant Intrusion	Attendants are able to activate intrusion towards MASI terminals.
Attendant Override	Attendants are not able to activate override towards MASI terminals..
Attendant Recall	MASI terminals cannot activate attendant recall.
Attendant Remote Trunk Group Select	Attendants cannot use this feature to select MASI remote trunks
Attendant Return Call	Operates normally if a MASI terminal is the called party.
Attendant Serial Call	Serial calls are denied if the calling party is an MMCX interface.
Attendant Straightforward Outward Completion	The attendant is able to complete calls to Communication Manager trunks for MASI terminals.
Attendant Through Dialing	The attendant can use Through Dialing to pass dial tone to MASI terminals.
Attendant Timers	Attendant timers work the same no matter what kind of terminal is involved..
Attendant Trunk Group Busy/ Warning Indicators	You cannot administer Busy/Warning indicators for MASI trunks because they are not standard Avaya Communication Manager trunks. However, you can administer these indicators for the trunk group administered for MASI paths.

Features	Constraints
Attendant Trunk Identification	The attendant is not able to identify the trunk name via button pushes.

Basic features

Features	Constraints
Abbreviated Dialing	A Communication Manager station can enter an MMCX extension in an AD list. However, MASI terminals cannot use AD.
Administered Connections	MASI terminals must not be the originator nor the destination of an administered connection.
Automatic Callback	Automatic callback does not work towards a MASI terminal.
Automatic Circuit Assurance	You must not administer a MASI terminal as an ACA referral destination. You cannot administer ACA for MASI remote trunks.
Busy Verification of Terminals and Trunks	You cannot use Busy Verification for MASI terminals or remote trunks.
Call Detail Recording	CDR Account Code Dialing and Forced Entry of Account Codes are not supported for MASI terminals.
Call Park	The attendant can park calls at the extension of a MASI terminal, but users can only retrieve these calls from a Communication Manager station, since MASI terminals cannot dial the Answer Back FAC.
Data Call Setup	AvayaCommunication Manager users cannot place data calls to MASI terminals.
Facility Busy Indication	You can use FBI to track the status of MASI terminals. The FBI button and indicator lamp must be on a Communication Manager station. You cannot use FBI to track MMCX interfaces.
Facility Test Calls	Avaya Communication Manager users cannot make test calls to MMCX interfaces.
Go to Cover	MASI terminals cannot activate this feature.
Leave Word Calling	The only valid LWC destination for a MASI terminal is AUDIX. You cannot administer SPE-based LWC. MASI terminals cannot send LWC messages to Avaya Communication Manager stations or to MASI terminals.
Loudspeaker paging	You can administer a MASI terminal as a code calling extension.
Malicious Call Trace	MASI terminals cannot initiate malicious call trace.

Features	Constraints
Message Retrieval	MMCX users can only retrieve messages through AUDIX messaging.
Music on Hold	Music on hold will only be available if an Communication Manager station has placed the call on hold.
Override	Executive override does not work towards MASI terminals.
Priority Calling	Priority calling is not supported for calls to or from MASI terminals.
Ringback Queueing	Ringback Queueing is not supported for MASI terminals.
Send All Calls	MMCX has an autonomous SAC function
Tenant Partitioning	All MASI terminals exist in tenant 1, and you cannot change the tenant number.
Time of Day coverage	As with all coverage, Communication Manager does not control coverage of the MASI terminal.
Transfer out of AUDIX	A MASI terminal cannot use *T to transfer from AUDIX to another MASI terminal.

Hospitality Features

Features	Constraints
Do Not Disturb	MASI terminals cannot activate Do Not Disturb.

Multimedia Features

Features	Constraints
Multimedia Call Handling	Avaya MMCH users are not able to make H.320 calls to MASI terminals over the MASI link. Calls between MMCX terminals and MMCH terminals are voice only.

Troubleshooting

About this task

Verify proper operation using the following commands and follow normal escalation procedures to resolve any failures detected by the demand test.

Procedure

1. Verify the DS1 trunk using the `test board <board location>` long command
2. Verify the ISDN Signaling Group using the `test signaling-group <group number>` command.

3. Also verify proper administration.
4. Verify the temporary signaling connection using the `test tsc-administered <group number>` command
5. Also verify proper administration.

Common Error Conditions

=

Error condition	Resolution
If the cable from an Avaya DEFINITY Server to the MMCX becomes disconnected	You should see alarms raised against ISDN-SGRP and UDS1-BD. In particular, you should observe ISDN-SGRP errors such as 769, 1793, and 257. To resolve, reconnect the cable and follow normal test procedures.
If the far-end path termination number is incorrect	You should observe MASI-PTH error 513. To resolve, correct administration using the MASI Path Parameters screen.
If the Layer 3 TSC is not administered properly or is out of service	You should observe errors (but no alarms) raised against TSC-ADM. Verify the signaling group administration and follow normal escalation procedures for TSC-ADM.
If the TSC fails to come up even through Layer 2 Signaling Group and below pass tests	you can run `test tsc-administered <group number>` to force a server heartbeat test, or simply wait 5 to 10 minutes for the link to recover. This situation might occur if the server running Communication Manager is rebooted or if the MASI interface is administered before the MMCX is properly administered.
if features are not working.	You might want to use the `busy port` and `release port` commands to unlock things

Video Telephony Solution

Use the Avaya Video Telephony Solution (AVTS) to enable videoconferencing for your desktop and group video communications.

Note:

AVTS is Avaya's newest, and currently available H.323 video solution. Some older systems may still use the older technology H.320 video solution, Multi-Media Call Handling (MMCH). For more information on MMCH, see *Multimedia Call Handling*.

The Avaya Video Telephony Solution enables Avaya Communication Manager to merge a set of enterprise features with Polycom's videoconferencing adjuncts. It unifies Voice over IP with video, web applications, Avaya's video enabled IP softphone, third party gatekeepers and other H.323 endpoints.

The following components are part of the Avaya Video Telephony Solution feature:

- Polycom VSX3000, VSX7000 and VSX8000 conferencing systems with Release 8.03 or later
- Polycom V500 video calling systems
- Polycom MGC video conferencing bridge platforms with Release 8.0.1. Release 7.5 of the MGC is not supported.
- Third party gatekeepers, including Polycom Path Navigator

You also need a system running Avaya Communication Manager Release 3.0.1, and Avaya IP Softphone release 5.2 with video integrator.

Starting with Communication Manager Release 3.1.2, you can use cumulative bandwidth management to set video bandwidth for the Avaya Video Telephony Solution. The Audio Call Admission Control (CAC) capability allows you to set maximum bandwidth between multiple network regions for audio calls. Video bandwidth can also be controlled in a similar way.

For more information, see also:

- *Avaya Video Telephony Solution Release 3.0 Networking Guide, 16-601423, Issue 1*
- *Video Telephony Solution Release 3.0 Quick Setup, 16-300310, Issue 3*
- *IP Softphone and Video Integrator Getting Started, 16-600748, Issue 2*

Note:

To configure the Polycom MGC-25 Video Conferencing Bridge Platforms with Avaya S8300D and S8510 Servers, see the procedures stated in the *Video Telephone Solution R3.0 Quick Set Up Guide, 16-300310, Issue 3, February 2007*

Related topics:

Multimedia Call Handling on page 358

Communication Manager SIP Video Infrastructure Enhancements

Note:

Communication Manager 6.0 as a SIP feature server implies that Communication Manager is configured with IMS enabled SIP signaling interfaces that are connected to the Session

Manager 6.0. The H.323 calls are not routed via the feature server and therefore, only SIP requirements impact feature server operation. From Release 6.0 Communication Manager is supported as an Access Element as well.

- Communication Manager 6.0 supports SIP video and audio shuffling optimization.
- Communication Manager reduces the total memory footprint of each SIP call leg that has video enabled by no longer storing a duplicate copy of far-end caps in the SIP user manager.
- Communication Manager does not allocate video structures internally when only audio media is present in the SDP for the initial dialog.
- Communication Manager indicates when the called party is a video enabled endpoint and hence allows video to be added when a called party is transferred or conferenced via sending a re-INVITE (no SDP) to trigger renegotiation of capabilities by both endpoints in the new call topology.
- Communication Manager has its capacity for SIP video calls set to 1/3 of the capacity for all SIP calls. This is the equivalent ratio of audio/video users with the current H.323 solution. This change ensures that SIP video capacity increases along with SIP audio capacity in a defined manner and as the work to increase audio calls is completed, additional video calls are supported.
- Communication Manager initiates video OLCs to H.323 MCUs on behalf of SIP endpoints.
- All existing Communication Manager H.323 functionality and compatibility with both Polycom and Meeting Exchange must be maintained. Versions of Polycom firmware as tested for CM 5.2 need to be verified against the Communication Manager 6.0 . The existing H.323 functionality also need to be verified against new One X Communicator 6.0 and Meeting Exchange firmwares.
- Communication Manager as a feature server supports negotiation between endpoints of a video fast-update mechanism using RTCP feedback as specified in RFC4585 and RFC5104.
- Communication Manager as a feature server supports negotiation between endpoints of a video flow-control (Temporary Maximum Media Bitrate Request) mechanism using RTCP feedback as specified in RFC4585 and RFC5104.
- Communication Manager implements simplified SIP call flows by removing the need to “black hole” video media in the initial SIP INVITE when direct media is enabled.
- Communication Manager as a feature server passes through any media sessions which it does not explicitly handle to tandem dialogs.

Administering the Avaya Video Telephony Solution

Before you begin

You must complete the following actions before you can administer the Avaya Video Telephony Solution:

1. Type `display system-parameters customer-options` to view the System Parameters Customer-Options (Optional Features) screen. Page down till you see

the Maximum Video Capable Stations field and the **Maximum Video Capable IP Softphones** field. These two fields show up only if your system is licensed for the Avaya Video Telephony feature. Your Avaya license file must contain the RTUs that were purchased for **Maximum Video Capable Stations** field and the **Maximum Video Capable IP Softphones** fields

> ✱ **Note:**
>
> You must make sure that the value of the Maximum Video Capable Stations field allows for each station that you use. In addition, each single-point VSX system is considered to be one station, and each multipoint VSX system is considered to be three stations.

2. Type `change ip-network-region #` to view the IP Network Region screen. The following fields must be set to `y` on this screen:
   - **Intra-region IP-IP Direct Audio**
   - **Inter-region IP-IP Direct Audio**
   - **IP Audio Hairpinning**

About this task

The following steps are part of the administration for the Avaya Video Telephony Solution:

- Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems
- Configuring Polycom PathNavigator Gatekeepers
- Configuring video trunks between two Communication Manager systems
- Configuring the Maximum Bandwidth for Inter-Network Regions
- Checking bandwidth usage
- Administering Ad-hoc Video Conferencing

Related topics:

Configuring Video-Enabled Avaya IP Softphone Endpoints on page 349
Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems on page 350
Configuring Polycom PathNavigator Gatekeepers on page 353
Configuring video trunks between two Communication Manager systems on page 355
Configuring the Maximum Bandwidth for Inter-Network Regions on page 356
Checking bandwidth usage on page 357

Configuring Video-Enabled Avaya IP Softphone Endpoints

Procedure

1. Type the `display system-parameters customer-options` command and verify number on the **Maximum Video Capable IP Softphones**. This number is provided by the Communication Manager license file.
2. Type `change ip-codec-set x` command (where x is the chosen IP codec set) to set the following parameters:
    a. Allow **Direct-IP Multimedia** to`y`.
    b. **Maximum Call Rate for Direct-IP Multimedia** - the Call Rate is the combined audio and video transmit rate or receive rate. You can use this setting to limit the amount of bandwidth used for calls.
    If you select 768 Kbits, a maximum of 768 Kbits will be used to transmit and to receive audio and video.
    c. **Maximum Call Rate for Priority Direct-IP Multimedia** allows you to set the maximum call rate per call for priority users
    d. Repeat this step for each IP codec set that will be used for video.
3. Type **change cos** and scroll down till you find the **Priority IP Video** field. This must be set to `y` for each class of station that is given a Priority status.
4. Type `change ip-network-region x` command (where x is the chosen IP network region) to set the following parameters:
    a. **Intra-region IP-IP Direct Audio** to `yes`.
    b. **Inter-region IP-IP Direct Audio** to `yes`.
    c. **Security Procedures 1** to `any-auth`
    d. Repeat this step for each IP network region that will be used for video.
5. Type `add station` command to add an Avaya IP Softphone station, and set the following parameters for that station
    a. **IP Softphone** to `y`.
    b. **IP Video Softphone** to`y`.
    c. **IP Audio Hairpinning** to `y`.
    d. Repeat Step 5 for each video-enabled Avaya IP Softphone endpoint you want to configure.

Related topics:

Administering the Avaya Video Telephony Solution on page 347

Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems on page 350

Configuring Polycom PathNavigator Gatekeepers on page 353
Configuring video trunks between two Communication Manager systems on page 355
Configuring the Maximum Bandwidth for Inter-Network Regions on page 356
Checking bandwidth usage on page 357

Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems

Before you begin

You must know the following information:

- Maximum number of VSX and V500 systems on your network
- PIN for each VSX/V500 system. The default is the unit's serial number
- Polycom software key for each system
- Avaya option key for each system
- Whether the VSX system has the multipoint option or IMCU option
- IP address of the voice system

Procedure

1. Use the `display system-parameters customer-options` command to verify the **Maximum Video Capable Stations**.

   This number is provided by the Communication Manager license file. The **Maximum Video Capable Stations** is determined by using the following criteria

   - Each V500 system is considered to be one station
   - Each single-point VSX system is considered to be one station
   - Each VSX multipoint system is considered to be three stations
2. Use the `change ip-codec-set x` command (where x is the chosen IP codec set) to define the following wideband codecs
   - SIREN14-S96K (1 fpp, 20 ms)
   - G722.1-32K (1 fpp, 20 ms)
   - G.726A-32K (no silence suppression, 2 fpp, 20 ms)
   - G.711MU (no silence suppression, 2 fpp, 20 ms)
   - G.729A (no silence suppression, 2 fpp, 20 ms)
   - Set **Allow Direct-IP Multimedia** to `y`
   - Set **Maximum Call Rate for Direct-IP Multimedia** - the Call Rate is the combined audio and video transmit rate or receive rate. You can use this setting to limit the amount of bandwidth used for calls. For example, if you select 768 Kbits, a maximum of 768 Kbits will be used to transmit and receive

audio and video. Repeat this step for each IP codec set that will be used for video.

- **Maximum Call Rate for Priority Direct-IP Multimedia** allows you to set the maximum call rate per call for priority users

3. Use the `change ip-network-region x` command (where x is the chosen IP network region) to set the following parameters:
   - **Intra-region IP-IP Direct Audio** to `yes`
   - **Inter-region IP-IP Direct Audio** to `yes`
   - **Security Procedures 1** to `any-auth`
   - Repeat this step for each IP network region that will be used for video.
4. Use the `add station` command to add a station for the Polycom system to set the following parameters
   - **Type** to `H.323`
   - **Security Code** to the `pin` on the VSX or V500 system
   - **IP Video** to `y`
   - **IP Audio Hairpinning** to `y`.
5. If the VSX system has the multipoint option or IMCU option, perform the following steps:

   a. Use the **add station** command to add a second station for the Polycom system.

   b. Set **Type** to `H.323`.

   c. Set **Security Code** to the `pin` on the VSX.

      Make sure the security code is the same as the previous station. All three stations must have the same security code.

   d. Set **IP Video** to y.

   e. Repeat Steps a through e to create the third consecutive station

   f. Use the `change station xx` command (where xx is the first station you added for the Polycom system) to set Hunt-to Station to the second station you added for the Polycom system.

   g. Use the `change station xx` command (where xx is the second station you added for the Polycom system) to set Hunt-to Station to the third station you added for the Polycom system.

   h. Use the `change station xx` command (where xx is the third station you added for the Polycom system) to set Hunt-to Station to the first station you added for the Polycom system. All three stations must be in a circular hunt.
6. Install the Polycom system and connect it to your network.
7. Upgrade the Polycom system software.

8. Using a web browser, access the Polycom home page for the unit, and select **Admin Settings>Network>IP Network**.
9. Select the **Enable IP H.323** check box.
10. Select the **Display H.323 Extension** check box.
11. In the **H.323 Extension (E.164)** box, enter the station number you specified for this system on the Avaya Communication Manager system.
12. From the **Use Gatekeeper** box, select `Specify` with `PIN`.
13. In the **Gatekeeper IP Address** box, enter the IP address of the CLAN or PCLAN followed by `:1719` to specify the correct port that must be used.
14. In the **Authentication PIN** box, enter the security code you entered in Step 3.
15. In the **Number** box in the Gateway area, enter the extension you specified in Step 9.
16. In the **Type of Service** box in the Quality of Section area, select `IP Precedence`
17. In the **Type of Service Value** boxes (Video, Audio, and Far End Camera Control), enter the QoS values for the IP Network Region settings in which the VSX station belongs.
18. Select the **Enabled PVEC** check box
19. Select the **Enable RSVP** check box.
20. Select the **Dynamic Bandwidth** check box.
21. From the **Maximum Transmit Bandwidth** box, select the setting that matches the **Maximum Call Rate for Direct-IP Multimedia** setting you specified for the Avaya Communication Manager system
22. From the **Maximum Receive Bandwidth** box, select the setting that matches the **Maximum Call Rate for Direct-IP Multimedia** setting you specified for the Avaya Communication Manager system.
23. Complete the **Firewall** and **Streaming** sections as necessary
24. When finished, click the **Update** button.
25. Repeat the steps for each Polycom system.

Related topics:

Administering the Avaya Video Telephony Solution on page 347
Configuring Video-Enabled Avaya IP Softphone Endpoints on page 349
Configuring Polycom PathNavigator Gatekeepers on page 353
Configuring video trunks between two Communication Manager systems on page 355
Configuring the Maximum Bandwidth for Inter-Network Regions on page 356
Checking bandwidth usage on page 357

Configuring Polycom PathNavigator Gatekeepers

Procedure

1. Use the `change ip-codec-set 1` command to set the following parameters.
    - Allow **Direct-IP Multimedia** to y (page 2 of screen).
    - **Maximum Call Rate for Direct-IP Multimedia**. This setting is the combined audio and video transmit rate or receive rate for non-priority (normal) video calls. You can use this setting to limit the amount of bandwidth used for normal video calls. For example, if you select 384 Kbits, a maximum of 384 Kbits will be used to transmit and to receive audio/ video.
    - **Maximum Call Rate for Priority Direct-IP Multimedia**. This setting is the combined audio and video transmit rate or receive rate for priority video calls. You can use this setting to limit the amount of bandwidth used for priority video calls. For example, if you select 384 Kbits, a maximum of 384 Kbits will be used to transmit and to receive audio/ video.
2. Use the `change ip-network-region x` command (where x is the chosen IP network region) to set the following parameters:
    - **Intra-region IP-IP Direct Audio** to `no`
    - **Inter-region IP-IP Direct Audio** to `no`
    - **Security Procedures 1** to `any-auth` (page 2 of screen).
    - **Video Norm** (page 3 of screen) to the amount of bandwidth that you want to allocate for the normal video pool to each IP network region.
    - **Video Prio** (page 3 of screen) to the amount of bandwidth that you want to allocate for the priority video pool to each IP network region.
    - **Video Shr** (page 3 of screen). Specify whether the normal video pool can be shared for each link between IP network regions.

    Note:

    If one of the video bandwidth limits is in Kbits, and another video bandwidth limit is in Mbits, all of the video bandwidth limits will be converted to the same unit (that is, Kbits or Mbits).
3. Use the `change node-names ip` command to add an entry for the Polycom PathNavigator gatekeeper. Be sure to enter the IP address of the IP board for the gatekeeper.
4. Use the add signaling-group command to add a signaling group for the gatekeeper. Set the following parameters:
    - **Group Type** to `h.323`

- **IP Video** to `y`
- **Near-end Listen Port** to `1719`.
- **LRQ Required** to`y`.
- **Incoming Priority Video**. If you want all incoming calls to receive priority video transmissions, select y.
- **Far-end Node Name** to the name you entered for the gatekeeper in Step 3.
- **Far-end Listen Port** to `1719`.
- **Far-end Network Region** to the IP network region you specified in Step 2.
- **Direct IP-IP Audio Connections** to `y`.
- **IP Audio Hairpinning** to `y`.

5. Use the add trunk-group command to add a trunk group for the gatekeeper. Set the following parameters:
    - **Group Type** to `isdn`.
    - **Carrier Medium** to `H.323`.
    - Add members to this trunk group.
6. Use the `change signaling-group xx` command (where xx is the signaling group you added in Step 4) to set **Trunk Group** for **Channel Selection** to the trunk group you added in Step 5.
7. Create a route pattern to the gatekeeper.
8. Configure the gatekeeper.

Related topics:

Administering the Avaya Video Telephony Solution on page 347
Configuring Video-Enabled Avaya IP Softphone Endpoints on page 349
Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems on page 350
Configuring video trunks between two Communication Manager systems on page 355
Configuring the Maximum Bandwidth for Inter-Network Regions on page 356
Checking bandwidth usage on page 357

Configuring video trunks between two Communication Manager systems

Procedure

1. Use the `change ip-codec-set 1` command to set the following parameters.
   a. Set **Allow Direct-IP Multimedia** to `y` (page 2 of screen).
   b. Set **Maximum Call Rate for Direct-IP Multimedia** - the Call Rate is the combined audio and video transmit rate or receive rate.

      You can use this setting to limit the amount of bandwidth used for calls
   c. **Maximum Call Rate for Priority Direct-IP Multimedia** allows you to set the maximum call rate per call for priority users
2. Type `display route-pattern xxx`, where xxx is the number for the route pattern

   To enable multimedia, the **M** field under BCC value must be set to y. This will allow you to send multimedia calls over a specific trunk.

   It is possible to have video over trunks that do not have M field set for the BCC. Setting **M** on the BCC enables you to select the route that the route pattern that you should use.
3. Use the `change node-names ip` command to add an entry for the trunk.

   Be sure to enter the IP address of the CLAN or PCLAN of the other Communication Manager system
4. Use the `add signaling-group` command to add a signaling group for the video trunk. Set the following parameters:
   - **Group Type** to `h.323` or `sip`
   - **Priority Video** to `y`
   - **IP Video** to `y`.
   - **Near-end Listen Port** .
   - **LRQ Required** to `y`.
   - **Far-end Node Name**
   - **Far-end Listen Port**
   - **Far-end Network Region**
   - **Calls Share IP Signaling Connection** to `n`.
   - **Direct IP-IP Audio Connections** to `y`.
   - **IP Audio Hairpinning** to `y`.

5. Use the `add trunk-group` command to add a trunk group for the video trunk. Set the following parameters
   - **Group Type** to `isdn`.
   - **Carrier Medium** to `H.323`.
   - Add members to this trunk group.
6. Use the `change signaling-group xx` command (where xx is the signaling group you added in Step 3) to set **Trunk Group** for Channel Selection to the trunk group you added in Step 4.
7. Create a route pattern for the trunk group.

Related topics:

Administering the Avaya Video Telephony Solution on page 347
Configuring Video-Enabled Avaya IP Softphone Endpoints on page 349
Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems on page 350
Configuring Polycom PathNavigator Gatekeepers on page 353
Configuring the Maximum Bandwidth for Inter-Network Regions on page 356
Checking bandwidth usage on page 357

Configuring the Maximum Bandwidth for Inter-Network Regions

Procedure

1. Type `change ip-network region 1`.
   The system displays the IP Network Region screen
2. Page down till you see the page titled Inter Network Region Connection Management.
3. In the column named **Total**, you can specify the bandwidth across the network regions. In the column named **Video**, you specify how much of the total bandwidth is to be used by video calls. The following are the available options:
   a. To support audio only and no video, set the **Video** field to `0` and audio to a very high number.
   b. To support audio and video with no bandwidth management, set both the **Total** and **Video** fields to `No Limit`.
   c. To restrict audio bandwidth, and allow unlimited video bandwidth, set the **Total** field to the desired bandwidth. Set the **Video** field to `No Limit`.

d. To control both audio and video bandwidth, set the **Total** field to the total bandwidth available between network regions. Set the **Video** field to the maximum bandwidth that can be used by video.

   The **Video** field must be set to a value less than or equal to the **Total**

e. Set priority video to the maximum bandwidth that can be used exclusively by priority video users.

Related topics:

Administering the Avaya Video Telephony Solution on page 347
Configuring Video-Enabled Avaya IP Softphone Endpoints on page 349
Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems on page 350
Configuring Polycom PathNavigator Gatekeepers on page 353
Configuring video trunks between two Communication Manager systems on page 355
Checking bandwidth usage on page 357

Checking bandwidth usage

Procedure

Type `status ip-network-region`.
The system displays the Inter Network Region Bandwidth Status screen for a call that is up.

You can view the audio bandwidth usage on the first row.

You can view the normal video bandwidth usage on the second row.

You can view the priority video bandwidth usage on the third row.

Related topics:

Administering the Avaya Video Telephony Solution on page 347
Configuring Video-Enabled Avaya IP Softphone Endpoints on page 349
Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems on page 350
Configuring Polycom PathNavigator Gatekeepers on page 353
Configuring video trunks between two Communication Manager systems on page 355
Configuring the Maximum Bandwidth for Inter-Network Regions on page 356

Administering Ad-hoc Video Conferencing

About this task

Administer the Ad-hoc Video Conferencing feature to allow users to create video conference calls. From a two-party video call, a user can press the **Conference** button on their telephone, dial the number of a third party, and press **Conference** again to add the party to the video conference call. Additional parties, up to a maximum of six, can be added in the same way. If the originator or any party who joins the conference call has administered COS permissions for Ad-hoc Video Conferencing, the video feature is enabled for the call. The call is moved from a Communication Manager hosted audio-only conference to an external bridge multimedia conference

Procedure

1. On page 2 of the *System Parameters Customer-Options (Optional Features)* screen, ensure that the **Maximum Administered Ad-hoc Video Conferencing Ports** field is set to the number of ports available for Ad-hoc Video Conferencing.
2. On the *Class of Service* screen, ensure that Ad-hoc Video Conferencing is set to `y` for each class of user with Ad-hoc Video Conferencing privileges. Then assign the COS on the Station screen for the appropriate users.
3. On the *Video Bridge* screen, configure video bridges for Ad-hoc Video Conferencing

   For more detailed information on Ad-hoc Video Conferencing, see *Avaya Video Telephony Solution Networking Guide, 16-601423.*

Multimedia Call Handling

Multimedia Call Handling (MMCH) enables users to control voice, video, and data transmissions using a telephone and PC. Users can conduct video conferences and route calls like a standard voice call. They can also share PC applications to collaborate with others working from remote sites

Note:

MMCH is Avaya's older technology H.320 video solution. Avaya Video Telephony Solution is Avaya's newer, and preferred H.323 video solution. For more information on AVTS, see *Avaya Video Telephony Solution*.

Note:

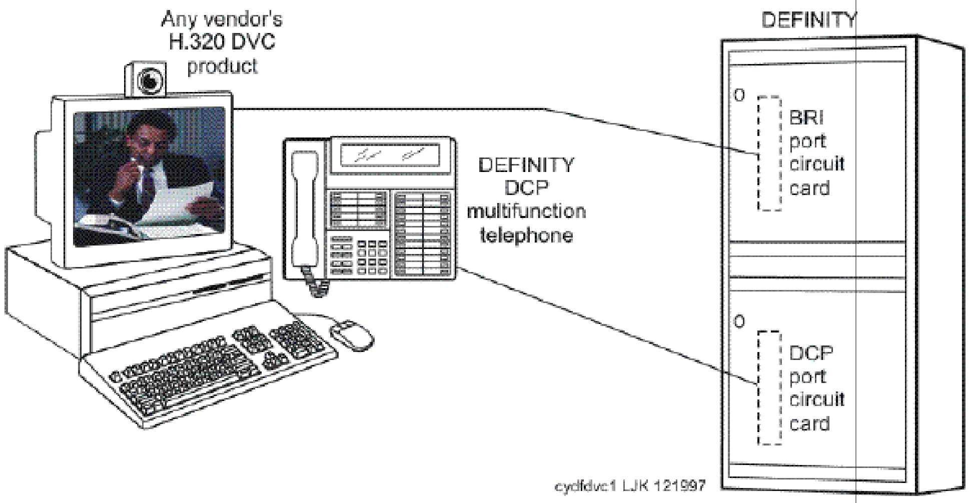
There are two distinct levels of functionality: Basic and Enhanced. The Basic mode of operation treats a standard-protocol H.320 multimedia call as a data call. If the call is redirected, it is converted to a voice call. As a voice call, certain features are enabled, such as coverage, voice mail, and multiparty video conferencing.

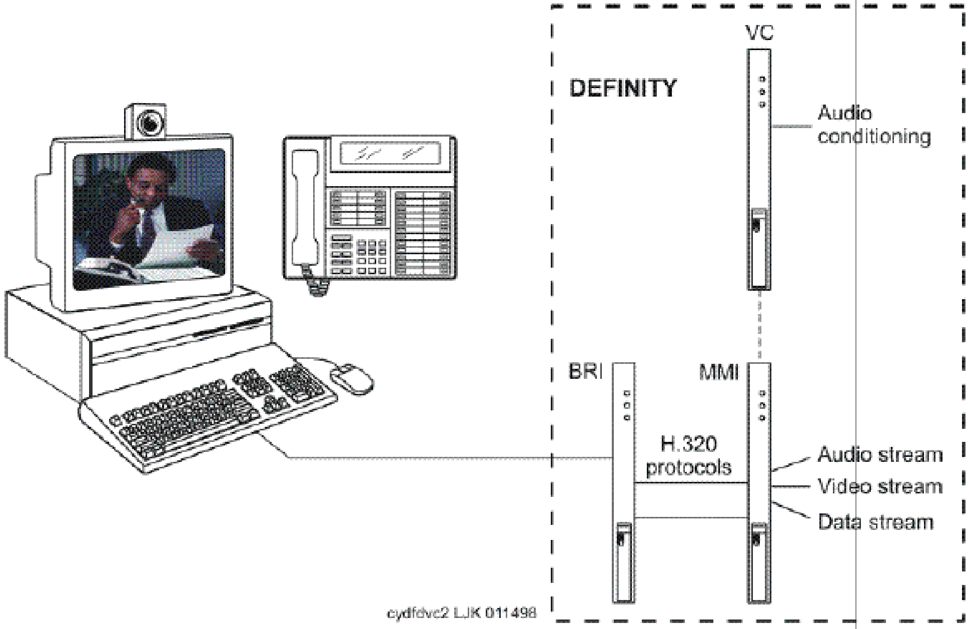
The Enhanced mode of operation allows a multifunction telephone to control a multimedia call as if it were a standard voice call. Spontaneous video conferencing, call forwarding, coverage, hold, transfer and park, along with many routing features, are available to multimedia calls. Both modes of operation allow data collaboration between multiple parties using the T.120 standard protocol.

Related topics:

Video Telephony Solution on page 345

Definitions: MMCH features and components

Features	Meanings
Multimedia call	A multimedia call, for MMCH, is one that conforms to the H.320 and T.120 suite of protocol standards. These standards allow video-conferencing packages from different vendors to communicate with one another. The capabilities of the individual multimedia-endpoint package can vary, however. • An H.320 call can contain voice, video and data. • The bandwidth for MMCH calls is limited to 2 B-channels  Any vendor's H.320 DVC product DEFINITY BRI port circuit card DEFINITY DCP multifunction telephone DCP port circuit card cydfdvc1 LJK 121997
Basic multimedia complex	A Basic multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone administered in Basic mode. With a Basic multimedia complex, users place voice calls at the multifunction telephone and multimedia calls from the multimedia equipped PC. Voice calls will be answered at the multifunction telephone and multimedia calls will alert first at the PC and, if unanswered, will next alert at the voice station. A Basic multimedia

Features	Meanings
	complex provides a loose integration of the voice station and H.320 DVC system.
Enhanced multimedia complex	An Enhanced multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone administered in Enhanced mode. The Enhanced multimedia complex acts as though the PC were directly connected to the multifunction telephone. Thus, voice call control, multimedia call control and call status are enabled at the telephone. An Enhanced multimedia complex provides a tight integration of the voice station and H.320 DVC system.
Multimedia endpoint	The multimedia endpoint is a user's PC that has been equipped with an H.320 multimedia package. The PC is physically connected to Avaya Communication Manager with a BRI line.  VC DEFINITY Audio conditioning BRI MMI H.320 protocols Audio stream Video stream Data stream cydfdvc2 LJK 011498
Enhanced mode service link	The service link is the combined hardware and software multimedia connection between the user's multimedia endpoint and the Avaya DEFINITY Server which terminates the H.320 protocol. The service link provides video, data, and, optionally, voice streams to augment the capabilities of the telephone and PC. A service link only applies to an Enhanced multimedia complex, never to a Basic multimedia complex. The service link is administered on the Station screen and can be either permanent or as-needed.

Basic Mode Operation

MMCH's two levels of functionality for a multimedia complex, Basic and Enhanced mode, are enabled either by administration on Communication Manager or by an mm-basic feature button or FAC.

- All voice-only calls originate at the voice station.
- All multimedia calls originate with the H.320 DVC system
- All incoming voice calls attempt to alert at the voice station and receive all standard voice call treatment.
- All incoming H.320 multimedia calls attempt to alert on the H.320 DVC system initially. If answered, a 2-way video call will result. The Basic multimedia complex voice station will not be involved in the call in any way.

  If the H.320 multimedia call is not answered at the H.320 DVC system and the Basic multimedia complex voice station has the **H.320** field administered to `y`, the call will:

  - Time out at the DVC system.
  - Alert at the associated voice station set as a voice-only call.
  - Receive all standard voice call treatment
- Call control depends on what type of call is being originated.
  - Video is received and controlled at the PC.
  - Voice is received and controlled at the telephone set.
- The voice station of a Basic multimedia complex must manually add their multimedia endpoint to a multimedia conference. There is limited support for multimedia feature interactions. A specific set of voice features work for multimedia calls.
- Service Links are not used by Basic mode complexes.
- A single number can be used to reach the Basic multimedia complex for voice or H.320 multimedia calls.

Related topics:

MMCH Settings Administration on page 366

Enhanced Mode Operation

The Enhanced multimedia complex provides a much more tightly coupled integration of the complex voice station and H.320 DVC system. In Enhanced Mode:

- Both multimedia and voice calls must originate at the telephone set.
- Voice and multimedia calls can be controlled at the telephone set.
- Conferencing is spontaneous and established just like a voice-only conference call.

- There is extensive support for multimedia feature interaction. Most voice features work the same for multimedia calls.
- Service Links can be either “permanent” or “as-needed”

Related topics:

MMCH Settings Administration on page 366

Physical Installation

The physical components necessary to utilize MMCH capabilities include:

- H.320 DVC systems that are BRI connected to the Avaya DEFINITY Server.
- Non-BRI multifunction telephones.
- Avaya TN787 MultiMedia Interface (MMI) and TN788 Voice Conditioner (VC) boards.
- A T.120 Extended Services Module (ESM) server (necessary only if you plan to do T.120 data collaboration). Connectivity of the ESM requires an additional TN787 along with a TN2207 DS1 circuit pack.

Dual Port Desktop

Both Basic and Enhanced multimedia complexes are dual-port desktops that consist of:

- A BRI-connected multimedia-equipped PC that supports the H.320 protocol.
- A non-BRI-connected multifunction telephone set.

  The PC and the multifunction telephone are individually wired to the Avaya DEFINITY Server. These two pieces of equipment can be administratively associated to form a Basic or ENHANCED multimedia complex

  MMCH works with any H.320 system that is fully H.320 compliant and operates at the 2B or 128K rate.

> **Note:**
>
> If you intend to share applications among users or whiteboard capabilities, the endpoint software you choose must also support the T.120 protocol.

The following endpoint-software packages have been tested:

- PictureTel PCS 50 & PCS 100, Release 1.6T.
- Proshare 2.0a, 2.1.
- Zydacron Z250 Ver. 2.02, Z350 Ver. 1.2 (With Netmeeting 2.0).

MMI & VC hardware

The MMCH feature requires the use of two additional circuit packs:

- Multi Media Interface (MMI) TN787J.
- Voice Conditioner (VC) TN788B.

The TN787 and TN788 are service circuit packs. The TN787 supports simultaneous operation of 16 2B H.320 calls. The TN788 supports the voice processing for 4 H.320 endpoints.

- These service circuit packs can be located in any Port Network.
- These packs do not require any translations as part of their implementation
- The MMI and VC circuit packs are resource circuit packs akin to the Tone Detector circuit packs.
- These circuit packs require no administration on Communication Manager and can be located in multiple port networks.

T.120 Data Collaboration Server

The Extended Services Module (ESM) provides T.120 data collaboration capability on a MMCH multipoint H.320 video conference.

- Each person in the conference who wants to participate in the data collaboration session, must have a personal computer with an H.320 video application that supports the T.120 protocol.
- The Avaya DEFINITY Server must have an ESM installed.

Installing ESM

About this task

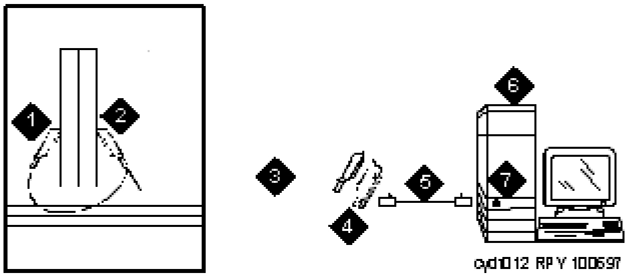
Use the following procedure and *Typical Multimedia Call handling ESM Connections* to connect to the ESM equipment:

Procedure

1. Install the TN2207 primary rate interface (PRI) circuit pack and the TN787 multimedia interface (MMI) circuit pack in the port carrier of the server for Avaya Communication Manager.

   Note:

   These two circuit packs should be co-located in the cabinet since they must be connected by a Y-cable on the back plane of the Avaya DEFINITY Server.



Typical Multimedia Call handling ESM Connections

a. Port B Y-cable connector to a TN787 multimedia interface (MMI) circuit pack
b. Port A Y-cable connector to a TN2207 PRI circuit pack
c. 25-pair Y-cable
d. 356A adapter
e. D8W cord connected to 356A adapter S/B port 8
f. Extended services module (ESM)
g. Port B on compatible primary rate interface (PRI) card

2. Record the circuit pack locations.
3. Connect the ESM Y-cable as shown.
4. Administer the DS1 Circuit Pack screen and the Signaling Group screen for the ESM (see *ESM T.120 Server Administration*).
5. Configure the ESM adjunct.

Planning MMCH

Before you begin

Questions that help you use Avaya Communication Manager for multimedia

- How many MMCH users are you going to have?
- How many multimedia calls do you expect to have at any given time?

  With the information above you can determine how many Voice Conditioner (VC) and Multimedia Interface (MMI) circuit packs you need.
- Will users need data collaboration capabilities? If so, you need to install the Extended Services Module (ESM).
- Which stations, hunt groups or vectors need early answer?
- Do you have ISDN-PRI trunks? It is possible to use separate DS1 trunks for data, but ISDN-PRI trunks are recommended.

Procedure

1. Purchase MMCH right-to-use.
2. Avaya — enable MMCH on System Parameters Customer-Options (Optional Features) screen.
3. Administer default multimedia outgoing trunk parameter selection on the Feature-Related System-Parameters Features screen.

4. Administer MMCH related feature access codes on the Feature Access Code (FAC) screen.
5. Install and administer hardware:
   a. Install MMIs, VCs and the ESM.
   b. Administer the ESM to ECS connection — DS1 Circuit Pack and Signaling Group screens.
   c. Establish maintenance parameters — Maintenance-Related System Parameters screen.
6. Administer multimedia complexes:
   a. Administer data modules — Data Module screen, or Data Module page of the Station screen.
   b. Administer stations as part of a multimedia complex, assign associated data module extension, multimedia mode, service link mode and appropriate multimedia buttons — Station screen
7. Administer early answer and H.320 flag for stations, the early answer flag for hunt groups, and the multimedia flag for vectors as appropriate.
8. Train end users.
9. Monitor traffic and performance.

Related screens

Screen Name	Settings
System Parameters Customer-Options (Optional Features)	Multimedia Call Handling (Basic) Multimedia Call Handling (Enhanced)
Feature Related System-Parameters	Default Multimedia Outgoing Trunk Parameter Selection (p.2)
Maintenance-Related System Parameters	Packet Bus Activated = y Minimum Maintenance Thresholds - MMIs, VCs
Data Module (type = 7500 or WCBRI)	Multimedia (p. 1) = y XID (p. 2) = n MIM Support (p. 2) = n
Station	MM Complex Data Ext (p. 1)

Screen Name	Settings
	H.320 Conversion (p. 2) Multimedia Early Answer (p. 2) Multimedia Mode (p.2) Service Link Mode (p.2) Feature Buttons (p.3) (optional)
Hunt Group	MM Early Answer (optional)
Call Vector	Multimedia (optional)
Feature Access Code (FAC)	Basic Mode Activation (p.5) Enhanced Mode Activation (p.5) Multimedia Call Access Code (p.5) Multimedia Data Conference Activation & Deactivation (p.5) The Multimedia Data Conference Deactivation FAC must be entered after you are active on a multimedia call. To enter the FAC: 1. Select Transfer 2. Receive a dialtone 3. Dial the FAC 4. Receive a confirmation tone. 5. Re-select the call appearance for the held multimedia call • Multimedia Multi-Address Access Code (p.5) • Multimedia Parameter Access Code (p.5
DS1 Circuit Pack (ESM Only)	Bit Rate=2.048. Line Coding=hdb3 Signaling Mode=isdn-pri Connect=pbx. Interface=network. Country Protocol=1 CRC=y. MMI Cabling Board
Signaling group (ESM Only)	Primary D-Channel

MMCH Settings Administration

System Parameters Customer-Options (Optional Features) screen

Ensure that the **Multimedia Call Handling (Basic)** field is y. This feature is provided via license file. To enable this feature, contact your Avaya representative

Feature-Related System Parameters screen

The default bandwidth for MMCH calls is defined on the Feature-Related System Parameters screen.

Note:

Originating a multimedia call with the mm-call button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen.

- This default parameter will be either 2x56 or 2x64.
- The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

Data Module screen

The H.320 DVC system should contain a BRI interface. You must connect this BRI interface to a port on a TN556 BRI circuit pack and administer it as a BRI data module.

- You can administer the data endpoint type as 7500 (recommended) or WCBRI.
- The fields for multimedia are the same on either screen.
- The administration for a Basic mode and an Enhanced mode data module are exactly the same.
- **Type** — Set the data module type to 7500 or WCBRI.
- **Multimedia** — This field appears on the Data Module screen only if MM is set to y on the System-Parameters Customer-Options (Optional Features) screen. Enter `y` to enable this data module to be multimedia compliant
- **MM Complex Voice Ext:** (display only) — This field contains the number of the associated telephone in the complex. This is a display-only field, and is blank until you enter the data module extension in the Station screen **MM Complex Data Ext** field. Once you have done that, these two extensions are associated as two parts of a multimedia complex.
- **XID and MIM Support** — Valid entries are y (default) and n. These fields must be set to `n`.

Station screen

After you have administered the BRI data module, use the Station screen to associate it with a voice station to screen a multimedia complex. This is a one-to-one relationship: you can administer only one station and one data endpoint per multimedia complex. Neither the voice station, nor the data endpoint can be a member of another multimedia complex.

Note:

A BRI station cannot be part of a multimedia complex

H.320 Conversion — Valid entries are y and n (default). This field is optional for non-multimedia complex voice stations and for Basic multimedia complex voice stations. It is mandatory for Enhanced multimedia complex voice stations. Because the system can only handle a limited number of conversion calls, you might need to limit the number of telephones with H.320 conversion. Enhanced multimedia complexes must have this flag set to y.

For non-multimedia complex voice stations, setting this field to y allows H.320 calls to convert to voice and alert at the stand-alone voice station. If the call is unanswered at the voice station, the call will follow standard voice treatment. Any subsequent station that is reached in the routing of this call, that is, coverage points, forwarded destinations, call pickup members, and so forth, do not need to have the **H.320** field enabled. The **H.320** field is only needed at the first station that might receive the H.320 call.

For Basic multimedia complex voice stations, setting this field to y allows H.320 calls to convert to voice and alert at the Basic multimedia complex voice station after an attempt has been made to offer the call to the H.320 DVC system. If the call is unanswered at the H.320 DVC system, the call will alert at the voice station after 5 seconds or after the administered number of rings as specified in the voice station's coverage path. If the call is unanswered at the voice station, the call will follow standard voice treatment. Any subsequent station that is reached in the routing of this call, that is, coverage points, forwarded destinations, call pickup members, and so forth, do not need to have the **H.320** field enabled. The **H.320** field is only needed at the first station that might receive the H.320 call.

Service Link Mode - The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and the Avaya DEFINITY Server which terminates the H.320 protocol. A service link is never used by a Basic mode complex H.320 DVC system. Connecting a service link will take several seconds. When the service link is connected, it uses MMI, VC and system timeslot resources. When the service link is disconnected it does not tie up any resources. The Service Link Mode can be administered as either as-needed or permanent as described below:

- As-Needed - Most non-call center multimedia users will be administered with this service link mode. The as-needed mode provides the Enhanced multimedia complex with a connected service link whenever a multimedia call is answered by the station and for a period of 10 seconds after the last multimedia call on the station has been disconnected. Having the service link stay connected for 10 seconds allows a user to disconnect a multimedia call and then make another multimedia call without having to wait for the service link to disconnect and re-establish.
- Permanent - Multimedia call center agents and other users who are constantly making or receiving multimedia calls might want to be administered with this service link mode. The permanent mode service link will be connected during the station's first multimedia call and will remain in a connected state until the user disconnects from their PC's multimedia application or the Avaya DEFINITY Server restarts. This provides a multimedia user with a much quicker video cut-through when answering a multimedia call from another permanent mode station or a multimedia call that has been early answered.

Multimedia Mode - There are two multimedia modes, Basic and Enhanced, as described below:

- Basic - A Basic multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone set. When in Basic mode, users place voice calls at the multifunction telephone and multimedia calls from the multimedia equipped PC. Voice calls will be answered at the multifunction telephone and multimedia calls will alert first at the PC and if unanswered will next alert at the voice station if it is administered with H.320 = y. A Basic mode complex has limited multimedia feature capability as described in *Basic Mode Operation* .
- Enhanced - An Enhanced multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone. The Enhanced mode station acts as though the PC were directly connected to the multifunction telephone; the service link provides the actual connection between the Avaya DEFINITY Server and the PC. Thus, voice and multimedia calls are originated and received at the telephone set. Voice and multimedia call status are also displayed at the telephone set. An Enhanced

mode station allows multimedia calls to take full advantage of most call control features as described in *Enhanced Mode Operation*.

Multimedia Early Answer — Valid entries are y and n (default). This field lets you set this telephone for early answer of multimedia calls. The system will answer the incoming multimedia call on behalf of the station and proceed to establish the H.320 protocol. After audio path has been established to the caller, the call will then alert at the voice station.

The station can then answer by going off-hook and will have immediate audio path. No hourglass tone will be heard by the answering party (see *Hourglass Tone*).

Example: An administrative assistant who does not have a multimedia PC, but might get multimedia mode calls from forwarding or coverage, might want to set the H.320 flag to y and the early answer flag to y on their voice station. This allows any multimedia call to be presented to the station with immediate voice path rather than hourglass tone. The answered call could then be transferred as voice to voice mail or transferred as multimedia to a user equipped with a multimedia endpoint.

Related topics:

Basic Mode Operation on page 361
Enhanced Mode Operation on page 361
Hourglass Tone on page 378

Assigning Multimedia Buttons

About this task

There are six new multimedia specific buttons that can be added to a voice station. Most of them can be placed on any voice station, whether it is part of a Basic multimedia complex, an Enhanced multimedia complex or not part of any multimedia complex. Two feature buttons, **mm-basic** and **mm-pcaudio**, can only be placed on stations which are part of an Enhanced multimedia complex. All of the multimedia specific feature buttons have a corresponding feature access code except **mm-pcaudio** and **mm-cfwd**.

Procedure

1. Use the mm-pcaudio feature via the button.
2. Use the **mm-cfwd** button to replace the standard `call forward` FAC followed by the `multimedia call` FAC.
3. Press the **mm-call** button followed by the destination extension digits. If the user has a speakerphone the user can simply press the **mm-call** button, which preselects an idle call appearance, followed by the destination extension digits.

   This **mm-call** button can exist on any voice station. Most multimedia enabled users will want an **mm-call** button. This button (or its corresponding FAC) must be used to indicate that the user is placing a multimedia mode call. To place a multimedia mode call the user would go off-hook, select an idle call appearance.

The **mm-call** button lamp lights when you press this button during call origination. The lamp also lights to indicate that the selected call appearance is a multimedia mode call.

4. Toggle between Basic and Enhanced mode to change the station's administered Multimedia mode.

   This **mm-basic** button is only allowed on the voice station of a multimedia complex. The **mm-basic** button toggles a station between Basic and Enhanced modes. This button can NOT be used to change the station's multimedia mode when the station has an active multimedia call appearance.

   When in Basic mode this field on the Station screen will show basic. When in Enhanced mode this field on the Station screen will show enhanced. The current station Multimedia mode will be saved to translation when a save translation command is executed.

5. To switch the audio path to the PC while active on a call, press the **mm-pcaudio** button (if off-hook you can now hang up the handset).

   This **mm-pcaudio** button only works for an Enhanced multimedia complex voice station. When originating or receiving a multimedia call, the audio path is connected to the voice station's handset or speakerphone device. The **mm-pcaudio** button allows a user to switch the audio portion of any call to their PC's audio input/output device (if available).

   The **mm-pcaudio** button's status lamp will light up when the button is pushed to move the audio path to the PC and remain lit while the audio path is at the PC device.

   Note:

   If you are on a voice only call, the voice path will switch to the PC device but you will get muted or loopback video depending on the multimedia endpoint software

   As a user you can simply go off-hook on your voice station or press the speakerphone button to move the audio path of a multimedia call from the PC back to the voice station. Pressing the mm-pcaudio button while the status lamp is lit and the voice station's handset is on-hook will disconnect the user from the active call.

6. Press the **mm-datacnf** button from any voice station that is participating in a multimedia call and the status lamp will light up and alert the Avaya DEFINITY Server that you want to enable T.120 data collaboration with the other parties on the call.
   The button status lamp will also light for other participants in the multimedia call who have **mm-datacnf** buttons. Pressing this button from the voice station that enabled data collaboration on a multimedia mode call will deactivate the data session and revert to a voice and video call. If you are participating on a multimedia call with data collaboration, but did not initiate the data collaboration, and you press this button, the status lamp led will flash momentarily and the T.120 data services will not be terminated, (only the station that activated the collaboration session can

deactivate it). This button only works for stations connected to an Avaya DEFINITY Server equipped with an ESM adjunct.

7. Press the **mm-cfwd** button to allow a user to indicate that multimedia mode calls will be forwarded as multimedia mode calls to a specific forwarded-to destination. If voice call forwarding is active and multimedia call forwarding is not active then multimedia calls going off of the Avaya DEFINITY Server will be forwarded as voice only calls. The **mm-cfwd** button status lamp will be lit to indicate that multimedia call forwarding is activated. Pressing the **mm-cfwd** button when the lamp is lit will deactivate multimedia call forwarding.

   Note:

   Pressing the **mm-cfwd** button is the same as dialing the regular call-fwd FAC followed by the mm-call button or FAC followed by the desired forwarded-to extension digits.

8. Press the **mm-multinbr** button to allow origination of a multimedia call from any voice station.

   The **mm-multinbr** call button is similar to the **mm-call** button. It is used when the destination being dialed requires a different address for each of the 2 B-channels. An example of this is Central Office provided ISDN-BRI. This type of BRI line is provisioned with separate listed directory numbers for each B-channel. In order to make a 2B multimedia call to such a device, two sets of address must be entered. Originating a multimedia call with the **mm-multinbr** button will originate a call according to the Default Multimedia Parameters selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

Administering the ESM T.120 Server

About this task

From the system administration terminal:

Procedure

1. Type `list configuration all`.
   A list of the installed carriers, circuit packs, and ports appears.
2. Record the location (board number) of the MMI board cabled to the TN2207 slot and verify that all other required circuit packs are present.
3. Enter `add DS1 xxxxx`, (where xxxxx is the location of the TN2207 PRI circuit pack recorded in step 2).
   The DS1 Circuit Pack screen appears.

4. Set the **Name** field to `ESM DS1`.
5. Set the **Bit Rate** field to `2.048`

   The TN2207 DS1 must have a bit rate of 2.048, even if all other DS1 boards in the system are operating at 1.544. Verify the 24/32 channel switch on the circuit pack is in the 32 channel position
6. Set the **Line Coding** field to `hdb3`
7. Set the **Signaling Mode** field to `isdn-pri`.
8. Set the **Connect** field to `pbx`.
9. Set the **Interface** field to `network`.
10. Set the **Country Protocol** field to `1`.
11. Set the **CRC** field to`y`.
12. The **Idle Code** default is `11111111`.
13. The **DCP/Analog Bearer Capability** default is `3.1` kHz.
14. Set the **MMI Cabling Board** field to `xxxxx` (where xxxxx is the location of the TN787 MMI circuit pack recorded in step 2).

    This must be the slot for port B of the Y-cable.

    The **MMI Interface** field ESM appears.
15. Enter `add signaling-group` next.
    The Signaling Group screen appears.
16. Set the **Associated Signaling** field to`y`.
17. Set the **Primary D-Channel Port** field to `xxxx16` (where xxxx is the address of the TN2207 PRI circuit pack).
    for example: 1B0516
18. The **Max Number of NCA TSC** default is `0`.
19. The **Max Number of CA TSC** default is `0`.
20. **Trunk Group for NCA TSC** ____ (leave blank).
21. **Trunk Group for Channel Selection**____ (leave blank).
22. Logoff the terminal and then log back on the terminal to view your changes.

Troubleshooting ESM

To determine ESM link status, enter the following commands from the system administration terminal:

- `Status esm`
- `Status signaling-group`
- `List MMI`

Note:

When you move ESM circuit packs, you MUST remove the DS1 and signaling group translations. You cannot use the **`change circuit pack`** command.

When a vector is used to route video (56K/64K) calls to a hunt group comprised of data extensions, the vector must have the **Multimedia** field set to n. This field causes multimedia calls routed through the vector to receive early answer treatment prior to processing the vector steps. This provides a talk path to the caller for announcements or immediate conversation with an agent and starts network billing for the incoming call when vector processing begins.

Understanding the Multimedia Complex

1-number access

1-number access permits originating users to make voice or multimedia calls to a Basic multimedia complex by dialing the same number for either type of call. The number might be the voice station extension or the data module extension. If the incoming call is a voice call, Avaya Communication Manager directs it to the telephone. If the incoming call is 56K or 64K data call, Avaya Communication Manager recognizes it as such and sends it to the multimedia endpoint. Likewise, if a voice call is addressed to the data extension, the system recognizes this and directs the call to the voice station.

Calls originating on the same server as the Basic mode complex destination can always use 1-number access for voice or video. In order to take advantage of 1-number access for calls originating from a remote location, the incoming calls must arrive over ISDN-PRI trunks. If the system is setup with separate data non-PRI digital facilities multimedia calls must be made to the data extension.

AVD (alternate voice/data) trunk groups cannot be used to provide 1-number access with MMCH. If the AVD trunk group has a BCC of 0, all calls arriving over the AVD trunk to the Basic mode complex will be assumed to be voice calls. If the AVD trunk group has a BCC of 1 or 4, all calls arriving over the AVD trunk to the Basic mode complex will be assumed to be multimedia calls.

Related topics:
Administering ISDN-PRI Trunk Group on page 332
Administering MASI Trunk Groups on page 333

Originating voice calls

All voice calls are originated at the voice station.

Originating multimedia calls

For a Basic mode complex, multimedia calls are normally originated at the user's multimedia equipped PC. These multimedia calls use the associated station's COR/COS.

The voice station of a Basic multimedia complex can also use the mm-call button or FAC, and the mm-multinbr button or FAC to originate multimedia calls. When these methods are used, a multimedia call is originated from the voice station. In order for the Basic multimedia complex to receive video, the user must make a call from the H.320 DVC system to the voice station of the complex or must make a multimedia call from the voice station to the H.320 DVC. This allows the station to spontaneously add themselves or other parties to a multimedia conference.

1. **H.320 DVC system GUI**. The normal way for a Basic multimedia complex endpoint to originate a multimedia call is through the vendor provided user interface. Generally, digits to dial are entered, speed is selected and the call originates from the DVC system. The voice station is not involved in such as origination.

   Any voice station can use the following mechanisms to originate a multimedia call from the voice station. For stations that are not part of a multimedia complex, video cannot be provided. For voice stations that are part of a Basic multimedia complex, video is not provided until a multimedia call is made from the complex's H.320 DVC system to the voice station or a multimedia call is made from the voice station to the H.320 DVC system. Video is automatically included for Enhanced multimedia complexes.

2. **mm-call** (Multimedia Call) button. If the station has an **mm-call** button administered, the user goes off-hook and selects the **mm-call** button. The user can select the mm-call button and then go off-hook. If the user has a speakerphone on the station, the user can originate the call simply by selecting the **mm-call** button. The speakerphone will automatically be placed off-hook and dialtone will be heard. Upon selection of the **mm-call** button, the mm-call status lamp (green LED) should become solid.

   The user now dials the destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, station busy indicators, etc. Originating a multimedia call with the **mm-call** button will originate a call according to the**Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either

2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

For calls with a bandwidth of 2B, use of the **mm-call** button to originate will cause the same destination address to be used for both channels of the 2B call. The section below on the mm-multinbr button/FAC provides information on originating a 2B call where the destination has a different address for each B-channel.

> **Note:**
>
> The mm-call feature button is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a multimedia call.

3. **Multimedia Call feature access code**. For stations that do not have an administered **mm-call** button, the Multimedia call feature access code can be used instead. The user goes off-hook on the station, waits for dialtone, then dials the MM-call FAC, receives dialtone again and then dials the call normally. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, station busy indicators, etc. Originating a multimedia call with the **mm-call** button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels. For calls with a bandwidth of 2B, use of the **mm-call** button to originate will cause the same destination address to be used for both channels of the 2B call. The section below on the mm-multinbr button/FAC provides information on originating a 2B call where the destination has a different address for each B-channel.

   > **Note:**
   >
   > The mm-call feature access code is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a multimedia call.

4. **mm-multinbr** (Multimedia Multi-number) button. The **mm-multinbr** button is similar to the **mm-call** button. It allows origination of a multimedia call from a voice station. It is used when the destination being dialed requires a different address for each of the 2 B-channels. An example of this is Central Office provided ISDN-BRI. This type of BRI line is provisioned with separate listed directory numbers for each B-channel. In order to make a 2B multimedia call to such a device, two sets of addresses must be entered.

   The user goes off-hook and selects the **mm-multinbr** button. The user can select the **mm-multinbr** button and then go off-hook. If the user has a speakerphone on the station, the user can originate the call simply by selecting the mm-multinbr button. The speakerphone will automatically be placed off-hook and dialtone will be heard. Upon selection of the **mm-multinbr** button, the mm-multinbr and mm-call (if present) status lamp (green led) should light steadily. The user now dials the first destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. The system will provide dialtone after the first address has been completed. The user now dials the second destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. After the 2nd address has been collected the mm-multinbr status lamp will go off.

Originating a multimedia call with the **mm-multinbr** button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

Note:

The mm-multinbr feature button is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

5. **Multimedia Multi-number Call feature access code**. For stations that do not have an administered **mm-multinbr** button, the Multimedia Multi-number call feature access code can be used instead. It allows origination of a multimedia call from a voice station. It is used when the destination being dialed requires a different address for each of the 2 B-channels. An example of this is Central Office provided ISDN-BRI. This type of BRI line is provisioned with separate listed directory numbers for each B-channel. In order to make a 2B multimedia call to such a device, two sets of addresses must be entered.

   The user goes off-hook and dials the MM-multinbr feature access code. Upon dialing of the MM-multinbr FAC, the mm-call (if present) status lamp (green led) should become solid. The user now dials the first destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. The system will provide dialtone after the first address has been completed. The user now dials the second destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc.

   Originating a multimedia call with the MM-multinbr FAC will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

   Note:

   The mm-multinbr FAC is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

6. **Multimedia parameter selection feature access code**. This FAC is used to originate a multimedia call that wishes to use a different bearer and bandwidth than the system default. For example, if the system has a default multimedia parameter of 2x64 and the user wishes to make a call to a destination that is known to only have 56K digital facilities, the MM parameter selection FAC can be used to select a bearer and bandwidth of 2x56 for this specific call.

   The MM parameter selection FAC can be used in conjunction with the mm-multinbr button or FAC to make a single or dual address multimedia call at the desired bearer and bandwidth. The user goes off-hook and dials the MM-parameter selection feature access code. Dialtone is returned. The user enters a single digit, 1 or 2, where 1 = 2x64, 2 = 2x56. All other digits will produce reorder. Dialtone is returned. Upon dialing of the MM-parameter selection FAC, the mm-call (if present) status lamp (green led) should become solid. The user can indicate a dual-address call at this point with the **mm-multinbr** button or FAC. The user now dials one or two sets of destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc

> **Note:**
>
> The mm-parameter selection FAC is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

7. Dialing sequences that include TACs, AAR, ARS, Authorization codes, CDR account codes, FRLs

    a. Single address with TAC

        i. Dial `mm-call` button or FAC, Hear dialtone

        ii. Dial `TAC`, Dial destination digits

    b. Dual address with TAC

        i. Dial **mm-multinbr** button or FAC, Hear dialtone

        ii. Dial `TAC`, Dial 1st dest. digits, Hear dialtone

        iii. Dial `TAC`, Dial 2nd dest. digits

    c. Single address with AAR/ARS

        - Dial **mm-call** button or FAC, Hear dialtone

        - Dial AAR/ARS, Dial destination digits

    d. Dual address with AAR/ARS

        i. Dial **mm-multinbr** button or FAC, Hear dialtone

        ii. Dial AAR/ARS, Dial 1st dest. digits, Hear dialtone

        iii. Dial AAR/ARS, Dial 2nd dest. digits

    e. Single address with AAR/ARS and authorization code

        i. Dial **mm-call** button or FAC, Hear dialtone

        ii. Dial AAR/ARS FAC, Dial destination digits, Hear stutter dialtone

        iii. Dial authorization code

    f. Dual address with AAR/ARS and authorization code

        i. Dial **mm-multinbr** button or FAC, Hear dialtone

        ii. Dial AAR/ARS FAC, Dial 1st dest. digits, Hear dialtone

        iii. Dial AAR/ARS FAC, Dial 2nd dest. digits, Hear stutter dialtone

    iv. Dial authorization code

g. Single address with TAC or AAR/ARS and CDR account code

    i. Dial **mm-call** button or FAC, Hear dialtone
    ii. Dial CDR FAC, Hear dialtone
    iii. Dial CDR account code, Hear dialtone
    iv. Dial TAC or AAR/ARS, Hear destination digits

h. Dual address with TAC or AAR/ARS and CDR account code

    i. Dial **mm-multinbr** button or FAC, Hear dialtone
    ii. Dial CDR FAC, Hear dialtone
    iii. Dial CDR account code, Hear dialtone
    iv. Dial TAC or AAR/ARS, Dial 1st dest. digits
    v. Dial TAC or AAR/ARS, Dial 2nd dest. digits

Receiving voice calls

Any voice calls directed to the voice or data extension of a Basic multimedia complex will ring at the voice station.

Receiving multimedia calls

Any data calls directed to the voice or data extension of a Basic multimedia complex will ring at the multimedia equipped PC if it is available. You can answer the multimedia call at the PC and voice and video will connect to the PC. If the data endpoint is unavailable, the system verifies that the telephone of the complex is administered with the H.320 field set to y. If so, the system converts the call to voice and sends it to the telephone of the multimedia complex, where the call then alerts.

Hourglass Tone

When a voice station answers a converted multimedia call, the answering party might hear different things depending on the nature of the originator. If the origination is directly from an H.320 DVC system or if the originator is an Enhanced mode complex on a remote server, an immediate audio path will not exist between the two parties. This is because the H.320 protocol must be established after the call is answered. It takes several seconds for the H.320 protocol to establish an audio path. During this interval the answering party will hear special ringback. When the audio path exists the special ringback will be removed and replaced with a short incoming call tone indicating that audio now exists. The combination of special ringback followed by incoming call tone is referred to as "hourglass tone." Hourglass tone is an indication to the answering party that they should wait for the H.320 call to establish audio.

Related topics:

MMCH Settings Administration on page 366

Early Answer

The answering party can administer their station to avoid hearing hourglass tone. With the Station screen **Early Answer** field set to y, the system answers the incoming multimedia call on behalf of the station and establishes the H.320 protocol. After audio path has been established, the call will then alert at the voice station of the Basic complex destination. The station can then answer by going off-hook and will have immediate audio path. No hourglass tone will be heard by the answering party.

If the **H.320** field is not set to y for the telephone of a Basic multimedia complex, H.320 calls alert at the multimedia endpoint until the caller drops. If an H.320 call is directed to a telephone with **H.320** set to n, the system denies the call.

You can assign H.320 conversion to any voice station.

Authorization

Multimedia complexes require the same types of authorization (COR/COS) as standard telephones. If a call is addressed to the voice extension, the system checks the COR/COS of the telephone, whether the call is voice-only or multimedia. If a call is addressed to the data extension, the system checks the COR/COS of the data endpoint. If the call is subsequently redirected to the voice station, the system does a second COR/COS check for the authorization of the voice station. Calls originated from the PC use the COR/COS of the voice station.

Adjunct Switch Applications Interface

ASAI is not expected to support call-association for data calls. Therefore Avaya does not recommend that you use ASAI for multimedia.

Administered Connection

Screen path: change administered-connection

This screen assigns an end-to-end Administered Connection (AC) between two access endpoints or data endpoints. The AC is established automatically by the system whenever the system restarts or the AC is due to be active. For information on how to access the endpoints, see *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Authorization and Barrier Codes

Basic Mode multimedia users or off-premises PC users might not be able to respond to prompts for authorization or barrier codes. Multimedia endpoints do not recognize the prompts.

An on-premises user might be able to use Remote Access and enter the entire digit string at once before launching the call, but it would be better to eliminate the need for such codes for multimedia users who need to call off premises.

Bridged Appearances

Voice users can bridge onto a call if the user has a bridged appearance of a voice member of the call.

Call Redirection

Calls directed to either member of the Basic multimedia complex are subject to redirection (coverage, forwarding). Avaya Communication Manager converts calls to voice before sending them to coverage. Calls redirected through call forwarding maintain multimedia status if forwarded from the data endpoint.

Conferencing

A multimedia conference can consist of multimedia and voice-only conferees. All multimedia conferees are added to a multimedia conference by a voice-terminal user on Communication Manager, who acts as the controller of the multimedia conference. When the controller is a Basic complex voice station, the controller must remain on the conference until all parties have joined. Once all endpoints are on the conference, the voice-terminal user can put the call on hold or drop, if the user wishes.

Video conferees can see only their local video and one other party. If more than two people are involved in a video conference, the person who is speaking is the one whose video appears to other conferees. The speaker’s video shows the previous speaker. This changes dynamically as the speaker changes.

Creating a multi-party video conference

About this task

All multimedia conferences must be controlled by a voice telephone. Multimedia conferees can be added by calling the voice telephone or by having the voice telephone make a multimedia call to other DVC endpoints. The controller can then conference together individual parties to create a multimedia conference.

Procedure

1. Determine who is going to be the conference controller.
2. At the appointed time, the conference controller calls his or her telephone from the multimedia endpoint by dialing the 1-number extension. Once this call is established, the controller conferences in other calls as if this were a voice conference. The controller continues to add conferees in this manner until all conferees have joined, or until the number of conferees reaches the administered limit.
3. The conference controller can also add voice or multimedia parties to the conference spontaneously. The controller presses **CONFERENCE**, makes a voice or multimedia call to a new party. To make a multimedia call, the controller must originate a call using the mm-call button or FAC or the **mm-multinbr** button or FAC. After the new party begins alerting, the controller can press **CONFERENCE** to add the party to the existing conference call on hold.

Coverage

Multimedia calls to a Basic mode complex are subject to the same coverage criteria as voice calls and follow the coverage path administered for the voice station of the Basic multimedia mode complex.

If a plain voice station or a Basic mode complex is the covering party, the answering voice station will receive audio only. If all voice stations in the coverage path have the Station screen Early Answer field set to n and the originator of the multimedia call was not a local Enhanced mode complex, the answering station will hear hourglass tone. If an Enhanced mode complex is the covering party, the answering voice station will receive voice and video.

If all voice stations in the coverage path have the Station screen **Early Answer** field set to `n` and the originator of the multimedia call was not a local Enhanced mode complex, the answering station will hear hourglass tone.

Coverage: Multimedia calls and off-net call coverage

If the principal station's coverage path include a remote coverage point, the multimedia call will cover off-switch as voice only. If the call is unanswered off-switch and proceeds to the next coverage point on-switch, the multimedia nature of the call is preserved.

Coverage: Multimedia calls and coverage to voice mail

Voice mail systems such as AUDIX are typically the last point in a coverage path and are usually implemented as a hunt group. In order to guarantee that the originator of an H.320 multimedia call hears the voice mail greeting, the hunt group that defines the list of voice mail ports should have the **Early Answer** field on the hunt group set to y. This field will have no effect on voice calls to the voice mail system.

Call Detail Recording

Each channel of a 2-channel call generates a separate CDR record.

Data Collaboration

Once you have established a multi-point video conference, multi-point T.120 data collaboration can be enabled for that call. This will allow all video parties on the current conference to collaborate.

T.120 Data conferencing is made possible through the Extended Services Module (ESM) server, which is an adjunct to Avaya Communication Manager. Up to six parties can participate in a single data conference, and up to 24 parties can use the ESM facilities for data collaboration at any given time.

Adding data sharing to a video conference

Procedure

1. Set up a multimedia conference.
2. Once a multimedia call is active, any voice station in the conference, can initiate data collaboration by pressing the **mm-datacnf** button. Or, to use the feature access code to initiate a data conference, press the **Transfer** button.

   A second line-appearance becomes active and you hear the dial tone.
3. Dial the multimedia data conference feature access code.
   Confirmation tone is heard and the system automatically reselects the held call appearance of the multimedia conference. Avaya Communication Manager will select a data rate which is acceptable to all H.320 DVC systems in the current call. If the system does not have sufficient ESM server resources available for all parties currently in the call, the activation of T.120 data sharing will be denied. The mm-datacnf status lamp will flash denial or the mm-datacnf FAC will produce reorder.

   > **Note:**
   >
   > Each H.320 DVC system in the conference call is joined to the data conference. On many DVC systems, the provided GUI can prompt the user with a dialog box, requesting the user to select a specific conference to join. With MMCH, there should only be one conference available to select.
4. You must now use the PC’s GUI to begin application sharing.

   The method for beginning application sharing or file transfer is different for each H.320 multimedia application. One of the H.320 DVC systems activates data sharing from the H.320 DVC vendor provided GUI. See your H.320 DVC system documentation for details.

The same H.320 DVC system as in step 4, opens an application, whiteboard, etc. to share and the image of the application is displayed on all H.320 DVC systems in the conference. For details on how multiple users can control the shared application, see the vendor provided documentation for your specific H.320 DVC system.

5. To end the data collaboration session and retain the voice/video conference, the station that selected the **mm-datacnf** button or FAC can press the **mm-datacnf** button or hit transfer and dial the mm-datacnf deactivation FAC.

Note:

As of this writing, many endpoints do not respond correctly to ending the data collaboration session and retaining voice/video. Some H.320 DVC systems drop the entire call. Avaya recommends that once T.120 data sharing has been enabled for a conference, that it remain active for the duration of the conference call. When all endpoints have dropped from the call, the T.120 resources will be released.

Joining a multimedia conference after T.120 data sharing has been enabled

If a multimedia conference with T.120 data sharing is already active and it is desired to conference in a new video endpoint, the new video endpoint can be conferenced into the existing call. The new endpoint will be allowed into the data conference if there exists sufficient ESM server resources for the new endpoint. The new endpoint will get voice/video and data sharing if the new endpoint supports the multi-layer protocol (MLP) data rate chosen by the system when T.120 data collaboration was activated. If the endpoint does not support the pre-existing MLP data rate, the new endpoint will only receive voice and video.

Single server or switch data collaboration

When all parties involved in data collaboration conference are located on the same physical Avaya S8XXX Server, there is no restriction on the type of user. The parties can be any combination of Enhanced multimedia complexes, Basic multimedia complexes, or stand-alone H.320 DVC systems.

Multi-switch data collaboration

When all parties involved in data collaboration conference are not located on the same physical Avaya S8XXX Server, the parties located on the Avaya server hosting the data conference (i.e. the server which activated **mm-datacnf**) can be any combination of Enhanced multimedia complexes, Basic multimedia complexes or stand-alone H.320 DVC systems.

Note:

All parties on remote servers must not be Enhanced multimedia complexes: they must be Basic multimedia complexes or stand-alone H.320 DVC systems.

Prior to originating or receiving a multimedia mode call, the **mm-basic** feature button or feature access code can be used to dynamically change an Enhanced mode complex into a Basic mode complex and back again.

Forwarding voice/multimedia calls

About this task

In Basic mode you can forward calls from either the telephone or the multimedia endpoint.

Procedure

1. At the PC's multimedia application, enter the call-forwarding feature access code (FAC).
2. Enter the forward-to number in the `Dialed Number` field on the endpoint software.
3. Click the **Dial** button (or equivalent)

   Note:

   The PC multimedia software will probably respond with a message that the call failed, since it does not recognize the FAC. In fact, Avaya Communication Manager does receive the message, and forwards all multimedia calls addressed to the 1-number.

   If a call is forwarded from the telephone, the call converts to voice first. If using the multimedia endpoint to forward, the calls arrive at the forwarded-to extension as a data call. Such calls continue to ring until answered or abandoned, rather than follow a coverage path.

   Users can forward calls from the multimedia endpoint using the call forward FAC. You can also assign a call-forward button at the voice station to forward calls for the data endpoint. If a Basic multimedia complex has console permissions, that user can forward calls for others by dialing the FAC, the data extension, and then the forwarded-to number.

Call Park

A voice-terminal user can park any active call, voice or multimedia, and unpark the call from another telephone. Users cannot park or unpark calls using multimedia endpoints.

Call Pickup

Users might need to answer a call that is ringing at a nearby desk. With Communication Manager, a user can answer a call that is ringing at another telephone in three ways:

- Use Call Pickup. With Call Pickup, you create one or more pickup groups. A pickup group is a collection, or list, of individual telephone extensions. A pickup group is the way to connect individual extensions together. For example, if you want everyone in the payroll department to be able to answer calls to any other payroll extension, you can create a pickup group that contains all of the payroll extensions.

  A user extension can belong to only one pickup group. Also, the maximum number of pickup groups might be limited by your system configuration.

  Using their own telephones, all members in a pickup group can answer a call that is ringing at another group member telephone. If more than one telephone is ringing, the system selects the extension that has been ringing the longest.

- Use Extended Call Pickup. With Extended Call Pickup, you can define one or more extended pickup groups. An extended pickup group is the way to connect individual pickup groups together.

  There are two types of extended pickup groups: simple and flexible. You administer the type of extended pickup groups on a system-wide basis. You cannot have both simple and flexible extended pickup groups on your system at the same time.

  Based on the type of extended pickup group that you administer, members in one pickup group can answer calls to another pickup group.

  For more information, see *Setting up simple extended pickup groups*, *Setting up flexible extended pickup groups*, and *Changing extended pickup groups*.

- Use Directed Call Pickup. With Directed Call Pickup, users specify what ringing telephone they want to answer. A pickup group is not required with Directed Call Pickup. You must first administer Directed Call Pickup before anyone can use this feature.

For more information, see *Setting up Directed Call Pickup*.

Consult

After a call is converted to voice, consult can be used when transferring or conferencing the call.

COR / COS

The Class of Restriction and Class of Service for H.320 calls originated from a 1-number complex are the same as those of the telephone in the complex.

Data Call Setup

Basic complex multimedia endpoints are BRI data endpoints, and can use data call-setup procedures as provided by the software vendor.

Data Hotline

Data Hotline provides for automatic-nondial placement of a data call preassigned to an endpoint when the originating server goes off-hook. Use for security purposes.

If endpoint software allows users to select the dial function without entering a number, the endpoint can be used for hotline dialing.

Dial Access to Attendant

Access to Attendant is blocked for a data call from a Basic mode multimedia endpoint.

Data Trunk Groups

Data trunk groups can be used to carry H.320 calls of a fixed (administered) bearer capability.

Hold

The voice station and multimedia endpoint of a Basic complex are each independent devices with respect to call control. When a Basic multimedia complex voice station executes hold only the voice station is held. If the user has conferenced their multimedia endpoint into a multimedia conference, activating hold will not disconnect the multimedia endpoint from the conference, it will only disconnect the Basic multimedia complex voice station. Executing hold with an Enhanced mode complex will fully disconnect voice and video from the current active call.

Hunt Groups using Basic Mode complexes

Since Basic mode complexes can receive point to point multimedia calls at the DVC system and voice calls to the station simultaneously, the voice station extension can be placed in any normal voice hunt group or ACD skill and the data extension can be placed in a simple hunt group made up of only data extensions.

Basic mode complex data extensions or stand-alone data extensions can be used to create simple data hunt groups. Data extensions are not allowed in ACD hunt groups. Avaya recommends that you do not mix voice and data stations in a hunt group.

If you want multimedia calls to hunt to multimedia endpoints (i.e. 2B point to point data hunting), put the data extension in the hunt group. If you place the voice extension in a hunt group, only voice calls hunt to that extension. Multimedia calls to a hunt group with a Basic mode voice station as the hunt group member will not be offered to the DVC system of the Basic mode complex. If either the voice or data extension of a Basic mode complex is busy, the entire complex is considered busy for hunting purposes.

In order to guarantee that all members of a voice hunt group or skill can receive voice or multimedia calls, all members should have the H.320 field on the Station screen set to y. Simple voice stations and Basic complex mode voice stations will receive voice only. Enhanced mode stations will receive voice and video.

The **MM Early Answer** field (on the Hunt Group screen) tells the system to answer the incoming multimedia call and establish audio before it reaches the first member of the hunt group. Thus, when the talk path is established, the caller is able to speak with an agent immediately. This is not necessary for hunt groups comprised of data extensions.

Hunting, Other considerations

Agents that are part of a Basic mode complex can dial a feature access code to remove themselves from availability (and to indicate that they are available again) from both the multimedia endpoint and the telephone independently. This allows the voice member or the data member to be individually made unavailable. To make the data extension unavailable, the agent must dial the FAC from the DVC system. CMS measurements can indicate unusually slow ASA, because of the time required for the system to establish early-answer before offering the call to an agent.

Hunting Call association (routing)

Typically incoming voice calls consist of 2 B-channel calls to the same address, to provide greater bandwidth and better video resolution. Avaya Communication Manager attempts to correctly pair up incoming calls and offer them as a unit to a single agent. MMCH uses call association to route both calls to the extension that answered the first call, regardless of how the call was routed internally.

Two 56K/64K data calls with the same calling party number to the same destination number are considered to be associated. The system makes every attempt to route both calls of a 2-channel call to the same answering party. If the first call terminates at a member of a hunt group, the second call does not have to hunt, but goes directly to the same member. In order for 2B multimedia calls to be correctly given to a single agent, incoming calls to the hunt group must have ANI information. The ANI information can be in the form of ISDN calling party number or DCS calling party number. Multimedia calls made on the same Avaya S8XXX Server as the hunt group are easily associated. If multimedia calls into a hunt group have incorrect ANI information (i.e. all calls from server X to server Y include the LDN for server X), then as the volume of calls increases, the number of mis-associated calls will increase. If multimedia calls into a hunt group have no ANI information, Communication Manager will never associate pairs of calls and all calls will be treated independently and routed to separate agents. This is not a recommended configuration.

Hunting with Multimedia vectors

Calls are often routed to hunt groups or skills via a vector. The existing VDNs and vectors which exist for routing voice calls can be used to route multimedia calls.

In order to use a vector for multimedia calls that will terminate to voice stations, you must set the **Multimedia** field on the Call Vector screen to y. This field has no effect on voice calls routing through the vector. This field will cause multimedia calls routed through the vector to receive early answer treatment prior to processing the vector steps. This provides a talk path to the caller for announcements or immediate conversation with an agent.

> **Note:**
>
> Vectors which have the **Multimedia** field set to y must eventually route to hunt groups, skills or numbers which are voice extensions. A vector with the **Multimedia** field set to y should never be set up to route to a hunt group or number which is a data extension.

When a vector is used to route video (56K/64K) calls to a hunt group comprised of data extensions, the vector must have the **Multimedia** field set to n.

Intercept Treatment

H.320 calls that receive intercept treatment are treated like other data calls. H.320 calls cannot be directed to an attendant for service because the attendant cannot have H.320 conversion service.

ISDN Trunk Groups

Avaya highly recommends that you use ISDN trunks for multimedia calls. ISDN PRI trunks allow complete 1-number access for an Enhanced multimedia complex. ANI provided over PRI trunks allows correct routing of multiple bearer channels to the correct destination device. ISDN also provides the bearer capability on a call by call basis which can be used to distinguish voice calls from multimedia calls.

Malicious Call Trace

If a malicious call terminates at a Basic multimedia complex endpoint, the user can dial the feature access code from the telephone to activate malicious call trace, followed by the extension of the multimedia endpoint. If the user does not dial the multimedia extension, MCT traces any call held on the telephone.

Message Waiting

Message Waiting indication is handled at the telephone. Because H.320 calls are converted to voice before going to coverage, all messages are voice only.

Night Service

You can use night service to direct calls to an alternate location when the primary answering group is not available. For example, you can administer night service so that anyone in your marketing department can answer incoming calls when the attendant is at lunch or has left for the day.

Once you administer night service to route calls, your end-users merely press a button on the console or a feature button on their telephones to toggle between normal coverage and night service.

There are five types of night service:

- Night Console Night Service — directs all attendant calls to a night or day/night console
- Night Station Night Service — directs all incoming trunk or attendant calls to a night service destination
- Trunk Answer from Any Station (TAAS) — directs incoming attendant calls and signals a bell or buzzer to alert other employees that they can answer the calls
- Trunk Group Night Service — directs incoming calls to individual trunk groups to a night service destination
- Hunt Group Night Service — directs hunt group calls to a night service destination

Remote Access

Communication Manager does not prevent Basic multimedia complexes from attempting to use remote access. However, these Basic mode endpoints will most likely not be able to dial the necessary codes.

Station Hunting

Basic mode data calls to endpoints that have an extension administered in the **Hunt-to-station** field hunt based on established hunting criteria. The call is converted to voice before station hunting.

Tenant Partitioning

Permission to make multimedia calls or add parties of any type to a conference is subject to standard tenant-partitioning restrictions.

Terminating Extension Groups

Basic mode data calls to a TEG are converted to voice and can terminate only at a voice endpoint. Effectively, Communication Manager treats the multimedia-complex extension as a voice-only endpoint.

Telephone Display

Display information for calls to or from a Basic multimedia complex contains the 1-number.

Enhanced Mode Operation

The Enhanced multimedia complex provides a much more tightly coupled integration of the complex voice station and H.320 DVC system. In Enhanced Mode:

- Both multimedia and voice calls must originate at the telephone set.
- Voice and multimedia calls can be controlled at the telephone set.
- Conferencing is spontaneous and established just like a voice-only conference call.
- There is extensive support for multimedia feature interaction. Most voice features work the same for multimedia calls.
- Service Links can be either “permanent” or “as-needed”

Related topics:
MMCH Settings Administration on page 366

Enhanced Mode MM Complex

The Enhanced multimedia complex provides a much greater unified and integrated interface for control of voice and multimedia calls. The multifunction voice station is used to control all calls, whether voice or multimedia. The H.320 desktop video system is used to present the video stream, data stream and (optionally) audio stream to the user. The H.320 desktop video system is not used for call control. The Enhanced multimedia complex allows the multifunction voice station to handle voice or multimedia calls in an almost identical manner. Each call appearance on the voice station can represent a voice or multimedia call, allowing multiple voice or multimedia calls to be present simultaneously on the station. The user can manage the separate call appearances without regard to the voice or multimedia nature of the specific call. The standard HOLD/TRANSFER/CONFERENCE/DROP actions can be applied to any call, without regard to the voice or multimedia nature of the call.

Originating Multimedia calls

The basic call sequence from an Enhanced mode complex is to originate a multimedia call and alert the destination. When the destination answers the call, the originating station's H.320 desktop video system will be alerted (that is, called by Communication Manager to establish the service link). If the H.320 DVC is not configured for auto-answer, the user must answer the H.320 calls via the DVC GUI. If the H.320 DVC is configured for auto-answer, no action is needed via the DVC GUI.

Note:

Avaya recommends, but does not require, that Enhanced mode complexes place their desktop video system into an auto-answer mode of operation.

If the far-end is providing a video signal, the 2-way video will be observed. If the destination is not providing a video signal (call was answered by a simple voice telephone), then loopback video will be provided at the Enhanced mode complex originator. The audio signal will exist at the handset of the voice telephone. The audio signal can be moved to the H.320 DVC system via activation of a **mm-pcaudio** button on the voice telephone.

Hourglass tone

The originating party might hear different things when the incoming multimedia call is answered depending on the nature of the answering party. If the call is being answered directly by an H.320 DVC system or if the answering party is an Enhanced mode complex on a remote server, an immediate audio path will not exist between the two parties. This is because the H.320 protocol must be established after the call is answered. It takes several seconds for the H.320 protocol to establish an audio path. During this interval the originating party will hear special ringback. When the audio path exists the special ringback will be removed and replaced with a short incoming call tone indicating that audio path now exists. The combination of special ringback followed by incoming call tone is referred to as "hourglass tone." Hourglass tone is an indication to the originating party that they should wait for the H.320 call to establish audio.

Originating voice calls

Voice calls are originated from the voice station of an Enhanced mode complex in the normal manner as for any voice station.

Originating multimedia calls

STATION, NOT the H.320 desktop video system. All multimedia originations require the user to indicate the multimedia nature of the call prior to providing any address digits. There are several different ways to originate a multimedia call from the voice station.

1. **mm-call** (Multimedia Call) button. If the station has an **mm-call** button administered, the user goes off-hook and selects the **mm-call** button. The user can select the **mm-call** button and then go off-hook. If the user has a speakerphone on the station, the user can originate the call simply by selecting the **mm-call** button. The speakerphone will automatically be placed off-hook and dialtone will be heard.

Upon selection of the **mm-call** button, the mm-call status lamp (green LED) will light steadily, indicating a multimedia call. The user now dials the destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, station busy indicators, etc. Originating a multimedia call with the mm-call button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels. For calls with a bandwidth of 2B, use of the **mm-call** button to originate will cause the same destination address to be used for both channels of the 2B call. The section below on the **mm-multinbr** button/FAC provides information on originating a 2B call where the destination has a different address for each B-channel.

Note:

The mm-call feature button is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a multimedia call.

2. Multimedia Call feature access code. For stations that do not have an administered **mm-call** button, the Multimedia call feature access code can be used instead. The user goes off-hook on the station, waits for dialtone, then dials the MM-call FAC, receives dialtone again and then dials the call normally. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, station busy indicators, etc.

   Originating a multimedia call with the **mm-call** button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

   For calls with a bandwidth of 2B, use of the mm-call button to originate will cause the same destination address to be used for both channels of the 2B call. The section below on the mm-multinbr button/FAC provides information on originating a 2B call where the destination has a different address for each B-channel.

   Note:

   The mm-call feature access code is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a multimedia call.

3. **mm-multinbr** (Multimedia Multi-number) button. The mm-multinbr button is similar to the mm-call button. It allows origination of a multimedia call from a voice station. It is used when the destination being dialed requires a different address for each of the 2 B-channels. An example of this is Central Office provided ISDN-BRI. This type of BRI line is provisioned with separate listed directory numbers for each B-channel. In order to make a 2B multimedia call to such a device, two sets of addresses must be entered.

   The user goes off-hook and selects the **mm-multinbr** button. The user can select the **mm-multinbr** button and then go off-hook. If the user has a speakerphone on the station, the user can originate the call simply by selecting the **mm-multinbr** button. The speakerphone will automatically be placed off-hook and dialtone will be heard. Upon selection of the **mm-multinbr** button, the **mm-multinbr** and **mm-call** (if present) status lamp (green led) should become solid. The user now dials the first destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. The system will provide dialtone after the first address has been completed. The user now dials the second destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. After the second address has been collected, the mm-multinbr status lamp will go off.

Originating a multimedia call with the **mm-multinbr** button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

Note:

The mm-multinbr feature button is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

4. Multimedia Multi-number Call feature access code. For stations that do not have an administered **mm-multinbr** button, the Multimedia Multi-number call feature access code can be used instead. It allows origination of a multimedia call from a voice station. It is used when the destination being dialed requires a different address for each of the 2 B-channels. An example of this is Central Office provided ISDN-BRI. This type of BRI line is provisioned with separate listed directory numbers for each B-channel. In order to make a 2B multimedia call to such a device, two sets of addresses must be entered.

   The user goes off-hook and dials the MM-multinbr feature access code. Upon dialing of the MM-multinbr FAC, the mm-call (if present) status lamp (green led) should become solid. The user now dials the first destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. The system will provide dialtone after the first address has been completed. The user now dials the second destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc.

   Originating a multimedia call with the MM-multinbr FAC will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

   Note:

   The mm-multinbr FAC is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

5. Multimedia parameter selection feature access code. This FAC is used to originate a multimedia call that wishes to use a different bearer and bandwidth than the system default. For example, if the system has a default multimedia parameter of

2x64 and the user wishes to make a call to a destination that is known to only have 56K digital facilities, the MM parameter selection FAC can be used to select a bearer and bandwidth of 2x56 for this specific call.

The MM parameter selection FAC can be used in conjunction with the **mm-multinbr** button or FAC to make a single or dual address multimedia call at the desired bearer and bandwidth. The user goes off-hook and dials the MM-parameter selection feature access code. Dialtone is returned. The user enters a single digit, 1 or 2, where 1 = 2x64, 2 = 2x56. All other digits will produce reorder. Dialtone is returned. Upon dialing of the MM-parameter selection FAC, the mm-call (if present) status lamp (green led) should become solid. The user can indicate a dual-address call at this point with the mm-multinbr button or FAC. The user now dials one or two sets of destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc.

Note:

The mm-parameter selection FAC is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

6. Dialing sequences that include TACs, AAR, ARS, Authorization codes, CDR account codes, FRLs
    a. Single address with TAC
        - Dial **mm-call** button or FAC, Hear dialtone
        - Dial TAC, Dial destination digits
    b. Dual address with TAC
        - Dial **mm-multinbr** button or FAC, Hear dialtone
        - Dial TAC, Dial 1st dest. digits, Hear dialtone
        - Dial TAC, Dial 2nd dest. digits
    c. Single address with AAR/ARS
        - Dial **mm-call** button or FAC, Hear dialtone
        - Dial AAR/ARS, Dial destination digits
    d. Dual address with AAR/ARS
        - Dial **mm-multinbr** button or FAC, Hear dialtone
        - Dial AAR/ARS, Dial 1st dest. digits, Hear dialtone
        - Dial AAR/ARS, Dial 2nd dest. digits
    e. Single address with AAR/ARS and authorization code
        - Dial mm-call button or FAC, Hear dialtone
        - Dial AAR/ARS FAC, Dial destination digits, Hear stutter dialtone
        - Dial authorization code

f. Dual address with AAR/ARS and authorization code

- Dial **mm-multinbr** button or FAC, Hear dialtone
- Dial AAR/ARS, Dial 1st dest. digits, Hear dialtone
- Dial AAR/ARS, Dial 2nd dest. digits, Hear stutter dialtone
- Dial authorization code

g. Single address with TAC or AAR/ARS and CDR account code

- Dial **mm-call** button or FAC, Hear dialtone
- Dial CDR FAC, Hear dialtone.
- Dial CDR account code, Hear dialtone
- Dial TAC or AAR/ARS, Dial destination digits

h. Dual address with TAC or AAR/ARS and CDR account code

- Dial **mm-multinbr** button or FAC, Hear dialtone
- Dial CDR FAC, Hear dialtone
- Dial CDR account code, Hear dialtone
- Dial TAC or AAR/ARS, Dial 1st dest. digits
- Dial TAC or AAR/ARS, Dial 2nd dest. digits

Answering multimedia calls

The user actions required to answer voice or multimedia calls at an Enhanced multimedia complex are identical if the H.320 DVC system is configured for auto-answer. If the H.320 DVC system is not configured for auto-answer an additional step is required. See Answering multimedia calls below.

Note:

Avaya recommends, but does not require, that Enhanced mode complexes place their desktop video system into an auto-answer mode of operation.

Answering voice calls

Incoming voice calls will alert at the voice station of the Enhanced multimedia complex in the normal manner. Standard alerting and call appearance flashing will occur. They are answered in the normal manner by selecting the alerting call appearance and going off-hook on the voice station.

Answering multimedia calls

Incoming multimedia calls will alert at the voice station of the Enhanced multimedia complex in the same manner as voice calls with one addition. If the alerting station has an administered mm-call button and the alerting call appearance is the selected call appearance (for instance, the red LED is lit, on the alerting call appearance), then the mm-call button status lamp will go on indicating that the call on the selected call appearance is a multimedia call.

The incoming multimedia call is answered in the normal manner by selecting the alerting call appearance and going off-hook on the voice station. If the H.320 DVC system for the answering party is configured for auto-answer, no other action is needed to complete the multimedia call. If the H.320 DVC system for the answering party is not configured for auto-answer, the H.320 DVC system will alert and must also be answered by the user.

Note:

Avaya recommends, but does not require, that Enhanced mode complexes place their desktop video system into an auto-answer mode of operation.

If the originating party is providing a video signal, then a complete 2-way multimedia call will exist. If the originating party is not providing a video signal, the answering party will receive loopback video. The audio signal will exist at the handset of the voice station. The audio signal can be moved to the H.320 DVC system via activation of a **mm-pcaudio** button on the voice station.

Hourglass Tone

The answering party might hear different things when the incoming multimedia call is answered depending on the nature of the originator. If the origination is directly from an H.320 DVC system or if the originator is an Enhanced mode complex on a remote server, an immediate audio path will not exist between the two parties. This is because the H.320 protocol must be established after the call is answered. It takes several seconds for the H.320 protocol to establish an audio path. During this interval the answering party will hear special ringback. When the audio path exists the special ringback will be removed and replaced with a short "incoming call tone" indicating that audio now exists. The combination of special ringback followed by incoming call tone is referred to as “hourglass tone”. Hourglass tone is an indication to the answering party that they should wait for the H.320 call to establish audio.

Early Answer

The answering party can administer their station in such a way as to avoid hearing hourglass tone. If the Station screen has set the **Early Answer** field to `y`, then the system will answer the incoming multimedia call on behalf of the station and proceed to establish the H.320 protocol. After audio path has been established, the call will then alert at the voice station of the Enhanced mode complex destination. The station can then answer by going off-hook and will have immediate audio path. No hourglass tone will be heard by the answering party.

Multiple call appearance operation

With an Enhanced mode complex all calls to or from the complex are controlled via the voice station. Each voice or multimedia call has its own call appearance which can be selected without regard for the nature of the call using the specific call appearance. This allows a multifunction station to control multiple voice or multimedia calls in exactly the same way they would control multiple voice calls.

As an example, a user can originate a simple voice call on the first call appearance. A multimedia call can then arrive on the second call appearance. The user activates **HOLD** on the first call appearance and selects the second call appearance to answer the multimedia call. The user can then activate **HOLD** on the second call appearance and reselect the first call appearance or select a third call appearance and originate another call.

A multi-party video conference

An Enhanced multimedia complex can create a spontaneous video conference in the same way that a spontaneous voice conference is created. Given an active call, the user activates the **CONFERENCE** button. This puts the current call on **HOLD** and activates a new call appearance. The user makes a multimedia call according to the instructions for originating a multimedia call and then selects **CONFERENCE** to combine or merge the two call appearances. This results in a 3-way conference.

If all three parties are video equipped, then a 3-way video conference results. Conference members see the current speaker on video. The current speaker sees the last speaker on video. If one of the parties is not video equipped, then a 3-way audio conference exists and the two video equipped parties have 2-way video. The **CONFERENCE** action can be repeated until 6 parties have been conferenced together. The 6 parties can be any mix of voice or video, local or remote parties.

Data Collaboration

Once you have established a multi-point video conference, multi-point T.120 data collaboration can be enabled for that call. This will allow all video parties on the current conference to collaborate. T.120 Data conferencing is made possible through the Extended Services Module (ESM) server, which is an adjunct to the Avaya DEFINITY Server. Up to six parties can participate in a single data conference, and up to 24 parties can use ESM facilities for data collaboration at any given time.

Joining a multimedia conference after T.120 data sharing has been enabled

If a multimedia conference with T.120 data sharing is already active and it is desired to conference in a new video endpoint, the new video endpoint can be conferenced into the existing call. The new endpoint will be allowed into the data conference if there exists sufficient ESM server resources for the new endpoint. The new endpoint will get voice/video and data sharing if the new endpoint supports the data rate chosen by the system when T.120 data collaboration was activated. If the endpoint does not support the pre-existing data rate, the new endpoint will only receive voice and video.

Activating HOLD while on a T.120 data collaboration conference

If an Enhanced multimedia complex is active on a multimedia call and the call has activated T.120 data collaboration, the user should be receiving voice/video and data. If the station places this existing call on hold, audio and video will be disconnected for the current call. The data collaboration portion of the call will remain intact and unaffected. While this T.120 data conference is on hold, the user will only be allowed to receive audio on all other call appearances. Thus a user is limited to one call appearance that has T.120 data collaboration active

Creating a multi-party video conference

About this task

Create a multi-party voice/video conference

Procedure

1. Enhanced mode complex station A originates a multimedia call to, or receives a multimedia call from, party B. Station A and party B have 2-way voice and video.
2. Station A, activates CONFERENCE
3. Station A originates a multimedia call (i.e. uses the mm-call button/FAC/etc.) and dials the party to be added, Enhanced multimedia complex C.
4. Party C, answers the call from station A.
5. Station A selects CONFERENCE to complete the 3-way conference. Parties A,B and C will be in a 3-way voice/video conference.

   Note:

   If party C is another Enhanced mode complex on the same Communication Manager server as station A, station A does not need to indicate a multimedia call prior to dialing the new party in step 3. While A consults with C, the call will be audio only. When A completes the conference in step 5, party C’s video will be activated.

   A multi-party video conference uses voice-activated switching to determine which parties are seen. The current speaker is seen by all other parties. The current speaker sees the previous speaker.

   Additional voice or video parties can be added by repeating these steps.

Data Sharing to a Video Conference

Procedure

1. Set up a multimedia conference.
2. Once a multimedia call is active, any member can initiate data collaboration by pressing the **mm-datacnf** button. Or, to use the feature access code to initiate a data conference, press the **Transfer** button.
   A second line-appearance becomes active and you hear dial tone. Dial the multimedia data conference feature access code. Confirmation tone is heard and the system automatically reselects the held call appearance of the multimedia conference. Avaya Communication Manager will select an MLP data rate acceptable to all H.320 DVC systems in the current call.

   If the system does not have sufficient ESM server resources available for all parties currently in the call, activation of T.120 data sharing will be denied. The mm-datacnf status lamp will flash denial or the mm-datacnf FAC will produce reorder.

3. Each H.320 DVC system in the conference call is joined to the data conference. On many DVC systems, the provided GUI might prompt the user with a dialog box, requesting the user to select a specific conference to join.

   With MMCH, there should only be one conference available to select.

4. The user must now use the PC's GUI to begin application sharing. The method for beginning application sharing or file transfer is different for each H.320 multimedia application.

   One of the H.320 DVC systems activates data sharing from the H.320 DVC vendor provided GUI. See your H.320 DVC system documentation for details.

5. The same H.320 DVC system as in step 4, opens an application, whiteboard, etc. to share and the image of the application is displayed on all H.320 DVC systems in the conference.

   For details on how multiple users can control the shared application, see the vendor provided documentation for your specific H.320 DVC system.

6. To end the data collaboration session and retain the voice/video conference, the station that selected the **mm-datacnf** button or FAC can press the **mm-datacnf** button or press Transfer and dial the mm-datacnf deactivation FAC.

   Note:

   Currently, many endpoints do not respond correctly to ending the data collaboration session and retaining voice/video. Some H.320 DVC systems drop the entire call. Avaya recommends that once T.120 data sharing has been enabled for a conference, that it remain active for the duration of the conference call. When all endpoints have dropped from the call, the T.120 resources will be released.

Single server or switch data collaboration

When all parties involved in data collaboration conference are located on the same physical Avaya S8XXX Server, there is no restriction on the type of user. The parties can be any combination of Enhanced multimedia complexes, Basic multimedia complexes or stand-alone H.320 DVC systems.

Multi-switch data collaboration

When all parties involved in data collaboration conference are not located on the same physical Avaya S8XXX Server, the parties located on the Avaya server hosting the data conference (i.e. the server which activated **mm-datacnf**) can be any combination of Enhanced multimedia complexes, Basic multimedia complexes or stand-alone H.320 DVC systems.

Note:

All parties on remote servers must not be Enhanced multimedia complexes: they must be Basic multimedia complexes or stand-alone H.320 DVC systems.

Prior to originating or receiving a multimedia mode call, the **mm-basic** feature button or feature access code can be used to dynamically change an Enhanced mode complex into a Basic mode complex and back again.

Voice station audio vs. H.320 DVC system audio

When an Enhanced mode complex originates or receives a voice or multimedia call, the call is originated with the station handset or answered with the station handset. The audio path will be through the handset. If the user's H.320 DVC system has speakers and a microphone, the user might wish to use the H.320 DVC system for audio in much the same manner as a built-in or separate telephone speakerphone. The user can move the station's audio to the H.320 DVC system by selecting an **mm-pcaudio** feature button on the voice station. There is no feature access code for this function.

The **mm-pcaudio** feature button works very much like a speakerphone on/off button. If the station is off-hook and selects **mm-pcaudio**, audio is directed to the PC DVC system. The switch-hook can be placed on-hook. If the handset is taken off-hook, the audio moves back to the handset. If the **mm-pcaudio** button is selected while audio is already on the DVC system and the handset is on-hook, this acts as a speakerphone off action and disconnects the current call.

The **mm-pcaudio** feature button can be used for voice as well as multimedia calls. If the **mm-pcaudio** feature button is selected while on a voice only call, the DVC system is alerted and brought into the call. No video will be transmitted or displayed. Audio will be directed through the PC DVC system.

Switching between Basic and Enhanced modes

There might be occasions when an Enhanced mode complex needs to switch to Basic mode operation temporarily. One example is when a user wishes to make a direct point to point multimedia call originated directly from the H.320 DVC. Basic mode operation allows this functionality at the expense of losing multimedia call handling capabilities (i.e. hold/xfer/conf). To switch from Enhanced mode to Basic mode, the station can either select a **mm-basic** feature button or dial the mm-basic feature access code. Both of these actions are valid only if the Enhanced mode station has no multimedia calls active.

When in Basic mode, the status lamp for the mm-basic button, if present, will be on solid. The **mm-basic** feature button acts as a toggle. If the status lamp is on, when the button is selected, the lamp will go off and the station will return to Enhanced mode. The mm-enhanced feature access code will set the state of the station back to Enhanced. Switching to Enhanced mode is only valid if the associated H.320 DVC system is idle.

Note:

Toggling between Basic and Enhanced mode changes the station's administered Multimedia mode. When in Basic mode this field on the Station screen will show basic. When in Enhanced mode this field on the Station screen will show enhanced. The current station Multimedia mode will be saved to translation when a `save translation` command is executed.

Forwarding of voice and multimedia calls

The Enhanced multimedia mode complex voice station can use the existing standard call forwarding mechanisms to activate forwarding for voice calls. If the forwarding destination is on the same server, then this will also forward multimedia calls as multimedia calls to the destination. If the forwarding destination is off-switch, multimedia calls will forward off-switch as voice-only calls. This is appropriate when the user will be at a location that is not able to receive multimedia calls.

To forward multimedia calls off-switch as multimedia calls, the user must activate multimedia call forwarding. This can be done with an **mm-cfwd** button or feature access code. The user can also activate standard voice call forwarding and select the **mm-call** button prior to entering the forwarding address.

Coverage

Multimedia calls to an Enhanced mode complex are subject to the same coverage criteria as voice calls and follow the coverage path administered for the voice Station of the Enhanced multimedia mode complex.

If a plain voice station or a Basic mode complex is the covering party, the answering voice station will receive audio only. If all voice stations in the coverage path have the Station screen **Early Answer** field set to n and the originator of the multimedia call was not a local Enhanced mode complex, the answering station will hear hourglass tone.

If an Enhanced mode complex is the covering party, the answering voice station will receive voice and video. If all voice stations in the coverage path have the Station screen Early Answer field set to n and the originator of the multimedia call was not a local Enhanced mode complex, the answering station will hear hourglass tone.

ForwardingVoiceMultimediaCalls2.dita

Multimedia calls and off-net call coverage

If the principal station's coverage path include a remote coverage point, the multimedia call will cover off-switch as voice only. If the call is unanswered off-switch and proceeds to the next coverage point on-switch, the multimedia nature of the call is preserved.

Multimedia calls and coverage to voice mail

Voice mail systems such as AUDIX are typically the last point in a coverage path and are usually implemented as a hunt group. In order to guarantee that the originator of an H.320 multimedia call hears the voice mail greeting, the hunt group that defines the list of voice mail ports should have the **Early Answer** field on the Hunt Group screen set to y. This field will have no effect on voice calls to the voice mail system.

Hunt Groups using Enhanced Mode Complexes

When creating hunt groups with Enhanced multimedia mode complexes, only the station extension should ever be entered as a hunt group member. Any hunt group or ACD skill can include the voice station of an Enhanced multimedia complex as a member. The data extension of an Enhanced mode complex should never be entered as any hunt group member. A hunt group or skill might have a mix of members that are stand-alone stations and Enhanced mode complex stations. In order to guarantee that all members of the hunt group or skill can receive voice or multimedia calls, all members should have the **H.320** field on the Station screen set to y. Simple voice stations will receive voice only. Enhanced mode stations will receive voice and video

The **MM Early Answer** field on the Hunt Group screen tells the system to answer an incoming multimedia call and establish audio before it reaches the first member of the hunt group. Thus, when the talk path is established, the caller is able to speak with an agent immediately.

Other considerations

CMS measurements can indicate unusually slow ASA, because of the time required for the system to establish early-answer before offering the call to an agent.

Call association (routing)

Typically incoming voice calls consist of 2 B-channel calls to the same address, to provide greater bandwidth and better video resolution. Communication Manager attempts to correctly pair up incoming calls and offer them as a unit to a single agent. MMCH uses call association to route both calls to the extension that answered the first call, regardless of how the call was routed internally.

Two 56K/64K data calls with the same calling party number to the same destination number are considered to be associated. The system makes every attempt to route both calls of a 2-channel call to the same answering party. If the first call terminates at a member of a hunt group, the second call does not have to hunt, but goes directly to the same member.

In order for 2B multimedia calls to be correctly given to a single agent, incoming calls to the hunt group must have ANI information. The ANI information can be in the form of ISDN calling party number or DCS calling party number. Multimedia calls made on the same server as the hunt group are easily associated. If multimedia calls into a hunt group have insufficient ANI information (i.e. all calls from server X to sever Y include the LDN for server X), then as the volume of calls increases the number of mis-associated calls will increase. If multimedia calls into a hunt group have no ANI information, Communication Manager will never associate pairs of calls and all calls will be treated independently and routed to separate agents. This is not a recommended configuration.

Multimedia vectors

Very often, calls are routed to hunt groups or skills via a vector. The existing VDNs and vectors which exist for routing voice calls can be used to route multimedia calls.

In order to use a vector for multimedia calls, you must set the **Multimedia** field on the Call Vector screen to y. This field has no effect on voice calls routing through the vector. This field will cause multimedia calls routed through the vector to receive early answer treatment prior to processing the vector steps. This provides a talk path to the caller for announcements or immediate conversation with an agent.

Note:

Vectors which have the **Multimedia** field set must eventually route to hunt groups, skills or numbers which are voice extensions. A vector with the **Multimedia** field set to y should never be set up to route to a hunt group or number which is a data extension

Interactions

Interactions are listed here only if the operation is different from standard.

Administered Connections

An Enhanced multimedia complex voice station can serve as the origination point or destination of an administered connection. If the Multimedia call feature access code is included in the administration of the administered connection, this will result in a video AC.

An Enhanced multimedia complex H.320 DVC system cannot serve as the origination point of an administered connection.

X-porting

You cannot use X in the **Port** field when administering a data module or the data endpoint in a multimedia complex. However, you can use this to administer the telephone.

Bridged Appearances

Enhanced multimedia complex voice station users can bridge onto a call if the user has a bridged appearance. If the bridged appearance is for a multimedia call, selecting the bridged appearance will result in a multimedia call.

Call Detail Recording

Each channel of a 2-channel multimedia call generates a separate CDR record that is tagged as data.

Call forwarding

Users cannot forward calls from a multimedia complex using multi-number dialing, either by mm-multnmbr button or feature access code.

Call Park

Any station can park a multimedia call, and unpark the call from another telephone. If a multimedia call is unparked by an Enhanced mode complex station, a multimedia call will result. Users cannot park or unpark calls using multimedia endpoints.

Call Pickup

Any member of a pickup group can answer a multimedia call after the call has begun alerting at a station call appearance. If the station picking up the call is an Enhanced mode complex station and the call is multimedia, a multimedia call will result. This is true for standard or directed call pickup.

Consult

After a multimedia call has been answered, consult can be used when transferring or conferencing the call.

COR/COS

The Class of Restriction and Class of Service for a multimedia call originated from an Enhanced multimedia complex are those of the voice station in the complex.

Data Call Setup

An Enhanced mode multimedia H.320 DVC system cannot originate calls from the DVC system. All calls, both voice or video are originated from the voice station.

Data Hotline

An Enhanced multimedia complex H.320 DVC endpoint cannot be used to originate a call for hotline dialing. In order to setup a video hotline function with an Enhanced mode complex, the hotline number administered for the voice station should include the Multimedia call feature access code.

Data Trunk Groups

Data trunk groups can be used to carry H.320 calls of a fixed (administered) bearer capability.

ISDN Trunk Groups

Avaya highly recommends that you use ISDN trunks for multimedia calls. ISDN PRI trunks allow complete 1-number access for an Enhanced multimedia complex. ANI provided over PRI trunks allows correct routing of multiple bearer channels to the correct destination device. ISDN also provides the bearer capability on a call by call basis that can be used to distinguish voice calls from multimedia calls.

Night Service

Incoming H.320 calls follow established night-service processing for data calls.

Remote Access

Communication Manager does not prevent Enhanced multimedia complexes from attempting to use remote access. However, these endpoints will most likely not be able to dial the necessary codes.

Station Hunting

Multimedia calls to Enhanced mode complex voice stations that have an extension administered in the hunt-to-station field hunt based on established hunting criteria. If the hunt-to-station is also an Enhanced mode complex station, a multimedia call will result when the call is answered.

Terminating Extension Groups

A multimedia call to a TEG can be answered by any member of the TEG. If the member answering the call is an Enhanced mode complex station, a multimedia call will result.

Telephone Display

Display information for calls to or from an Enhanced multimedia complex contains the display information associated with the voice station.

Troubleshooting

If one channel of a 2 B-channel call goes down, your choices are to continue with reduced transmission quality, or to hang up the call and start over. It is not possible to re-establish the second channel while the call is still active.

If you cannot share data with others, it might be that both parties do not have the same endpoint software. This is true for some data collaboration, but most whiteboard and file transfer software implementations are compatible.

Monitoring MMCH

This section briefly discusses some of the commands you can use to monitor multimedia complexes and conferences. The Maintenance manual for your Avaya server might discuss some of these commands and their output in more detail.

Action	Objects	Qualifier
display	station data module	xxxxx (extension) xxxxx (extension)
list	mmi measurements multimedia	multimedia-interface voice-conditioner esm endpoints [‘print’ or ‘schedule’] h.320-stations [‘print’ or ‘schedule’]
status	attendant conference conference conference data module station trunk esm	xxxx (console number) all xxx (conference ID) xxx (conference ID) endpoint (endpoint ID) xxxxx (extension) xxxxx (extension) (group number or group number/ member number)

Status commands

The `status` commands for data module, station, trunk, and attendant provide the conference ID and endpoint ID for any of these involved in an active multimedia conference.

The following fields specific to multimedia appear on the station General Status, Attendant, Data Module, and Trunk Group screens.

- **MM Conference ID** — This field appears only if the station is active on a multimedia conference. It displays the ID for the conference. Enter this number with the status conference command to get more information about this conference.
- **MM Endpoint ID** — This field appears only if the station is active on a multimedia conference. It displays the endpoint ID for the station. Enter this number with the status conference endpoint command to learn more about this endpoint's involvement in the conference.

List commands

The `list multimedia endpoints` command shows you all the multimedia data modules that exist in your system, and their associated telephones, if any. The `list multimedia H.320-stations` command shows you all the stations that are administered for H.320 conversion. The list multimedia `ip-stations` command shows you the administered IP stations/modules and whether they are registered.

Considerations

Each channel of a 2-channel BRI call takes one port on an MMI circuit pack. This alone limits the number of multimedia calls your system can handle. In addition, each conference takes one port on a voice-conditioner circuit pack. Also note that there is a limit to the total number of conversion calls the system can handle simultaneously. If you experience traffic problems after installing multimedia, you might want to reduce the number of stations that use H.320 conversion.

Chapter 13: Setting Up Telecommuting

Communication Manager Configuration for Telecommuting

Telecommuting emphasizes the ability to perform telephony activities while remote from Communication Manager. It is a combination of four features that permit you to remotely perform changes to your station's Coverage and Call Forwarding.

Note:

If you are operating in a Distributed Communications System (DCS) environment, you need to assign a different telecommuting-access extension to each Avaya S8XXX Server and tell your users which extension they should use. A user can set up call coverage from any of the DCS nodes, but needs to dial the telecommuting-access extension of the node on which their station is defined before using the feature access code. You can also set up telecommuting with an IP (internet protocol) telephone. See Adding an H.323 Softphone for more information.

- Coverage of Calls Redirected Off Net (Avaya IQON) allows you to redirect calls off your network onto the public network and bring back unanswered calls for further coverage.

  Note:

  If a call covers or forwards off-net and an answering machine answers the call, or it is directed to a cellular telephone and a cellular announcement is heard, the server views this call as an answered call. Communication Manager does not bring the call back to the server for further routing.

- The Extended User Administration of Redirected Calls feature allows you to change the direction of calls to your station. This activates the capability to have two coverage-path options. These two path options can be specified on the Station screen; however, unless the **Can Change Coverage** field is set to **y** on the Class of Restriction screen, the second path option cannot be populated. For information about this screen, see *Avaya Aura™™ Communication Manager Screen Reference*, 03-602878.
- The Personal Station Access feature gives you an extension number, a Merge feature access code, and a personalized security code, and tells you which office telephone you

can use. This allows you to take your telephone, as long as the telephones are the same type, anywhere on the same server running Communication Manager.

- The Answer Supervision feature provides supervision of a call directed out of the server either by coverage or forwarding and determines whether Communication Manager should bring the call control back to its server.

Preparing to configure telecommuting

About this task

You can also set up telecommuting with an IP (internet protocol) telephone or IP Softphone. For example, see Adding an H.323 Softphone for more information.

Procedure

1. For DCP/ISDN telecommuting, ensure that you have the following equipment:
   - Call Classifier — Detector
   - 1264-TMx software
   - Communication Manager extender — switching module or standalone rack mount (Digital Communications Protocol (DCP) or Integrated Services Digital Network (ISDN))
   - For more information about this equipment, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.
2. Verify the following fields on the System Parameters Customer-Options (Optional Features) screen are set to **y**.

   For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.
   - **Cvg Of Calls Redirected Off-Net**
   - **Extended Cvg/Fwd Admin**
   - **Personal Station Access**
   - **Terminal Translation Initialization (TTI)**

   If neither Communication Manager extender nor the System Parameters Customer-Options (Optional Features) fields are configured, contact your Avaya technical support representative.
3. Verify the telecommuting access extension is a direct inward dialing (DID) or a central office (CO) trunk destination for off-premises features to work.
4. Configure **TTI** for personal station access (PSA).

   For information about configuring TTI, see Personal Station Access setup.

5. Configure Security Violation Notification for Station Security Codes.

   For information about Security Violation Notification, see Security Violations Notification setup.

Configuring telecommuting example

About this task

In our example, we set up the telecommuting extension and enable coverage of calls redirected off-net.

Procedure

1. Enter `change telecommuting-access`.
2. In the **Telecommuting Access Extension** field, enter `1234`.

   This is the extension you are configuring for telecommuting.
3. Enter `change system-parameters coverage`.
4. In the **Coverage Of Calls Redirected Off-Net Enabled** field, enter `y`.

   See Telecommuting Access in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for information about and field descriptions on the Telecommuting Access screen.

Personal Station Access setup

Personal Station Access (PSA) allows you to associate the preferences and permissions assigned to your own extension with any other compatible telephone. When you request a PSA associate, the system automatically dissociates another extension from the telephone.

Preferences and permissions include the definition of terminal buttons, abbreviated dial lists, and class of service (COS) and class of restriction (COR) permissions assigned to your station. Extensions without a COS, such as Expert Agent Selection (EAS) agents or hunt groups, cannot use PSA.

PSA requires you to enter a security code and can be used on-site or off-site. Invalid attempts to associate a telephone generate referral calls and are recorded by Security Violation Notification, if that feature is enabled. If you interrupt the PSA dialing sequence by pressing the release button or by hanging up, the system does not log the action as an invalid attempt.

The disassociate function within PSA allows you to restrict the features available to a telephone. When a telephone has been dissociated using PSA, it can be used only to call an attendant, or to accept a TTI or PSA request. You can enable a dissociated set to make other calls by assigning a special class of restriction.

When a call that goes to coverage from a PSA-disassociated extension, Communication Manager sends a message to the coverage point indicating that the call was not answered. If the coverage point is a display telephone, the display shows `da` for “don't answer.” If the coverage point is a voice-messaging system, the messaging system receives an indication from Communication Manager that this call was not answered, and treats the call accordingly.

> **Note:**
>
> Once a telephone has been associated with an extension, anyone using the terminal has the capabilities of the associated station. Be sure to execute a dissociate request if the terminal can be accessed by unauthorized users. This is particularly important if you use PSA and DCP extenders to permit remote DCP access.

Preparing to set up Personal Station Access

Procedure

1. Verify that the **Personal Station Access** field is set to `y` on the Class of Service screen.

   For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.
2. Verify that the extension has a COS that allows PSA.

Setting up Personal Station Access example

About this task

In our example, we specify the TTI State, the Record PSA/TTI Transactions, the class of service, and the feature access codes set up for PSA.

Procedure

1. Enter `change system-parameters features`.
2. Complete the following fields.
   a. Enter `voice` in the **TTI State** field.
   b. (Optional) Enter `y` in the **Log CTA/PSA/TTI Transactions in History Log** field.

These fields display only when the **Terminal Translation Initialization (TTI) Enabled** field on this screen is set to `y`.

3. Enter `change cos`.
4. Enter `y` in the**Personal Station Access (PSA) 1** field.
5. Enter **`change feature-access-codes`**.
6. Complete the following fields.
   a. Enter `#4`in the **Personal Station Access (PSA) Associate Code** field.

      This is the feature access code you will use to activate Personal Station Access at a telephone.

   b. Enter `#3` in the **Dissociate Code** field.

      This is the feature access code you will use to deactivate Personal Station Access at a telephone.

   See Telecommuting settings changes for information on how to associate or disassociate PSA.

   See Enterprise Mobility User for information on how to set up the Enterprise Mobility User feature.

Related topics:

Enterprise Mobility User on page 196
Telecommuting settings changes on page 422

Placing calls from PSA-dissociated stations

About this task

You can allow users to place emergency and other calls from telephones that have been dissociated. To enable this:

Procedure

1. Assign a class of restriction (COR) for PSA-dissociated telephones.

   You do this on the Feature-Related System Parameters screen.

2. Set the restrictions for this COR on the Class of Restriction screen.

   If you want users to be able to place emergency calls from dissociated telephones, it is also a good idea to have the system send calling party number (CPN) or automatic number identification (ANI) information for these calls. To do this, you must set the **CPN, ANI for Dissociated Sets** field to `y` on the Feature-Related System Parameters screen.

Station Security Code setup

A Station Security Code (SSC) provides security to a station user by preventing other users from accessing functions associated with the user's station. Each station user can change their own SSC if they know the station's current settings.

You must create a system-wide SSC change feature access code (FAC) before users can change their SSC. You must also provide users with their individual SSC. A user cannot change a blank SSC.

Creating a Station Security Code example

About this task

In our example, we set the station security code for a user. For information about the screens referred in this topic, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Procedure

1. Enter `change feature-access-codes`.
2. Enter `#5` in the **Station Security Code Change Access Code** field.
3. Enter `change system-parameters security`.
4. Enter `4` in the `Minimum Station Security Code Length` field.

   This determines the minimum required length of the Station Security Codes you enter on the Station screen. Longer codes are more secure. If station security codes are used for external access to telecommuting features, the minimum length should be 7 or 8.
5. Enter `change station 1234`.

   This is the station extension you configured for telecommuting.
6. Enter `4321` in the **Security Code** field.

   See *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for information about and field descriptions on the Station screen.

   See Station Security Codes in *Avaya Aura™ Communication Manager Feature Description and Implementation*, (555-245-205) for a description of the Station Security Codes feature.

Assigning an Extender Password example

About this task

Communication Manager allows you assign an extender password to a user. You can assign one password for each Communication Manager port.

Use the Remote Extender PC in the server room to perform this procedure.

In this example, we will set a system-generated random password for a user named John Doe.

Procedure

1. Double-click the **Security** icon.
2. Double-click **User Password for User 01**.
3. Select **Enable Password** to enable the password.
4. Click **random**.

   This means that the password is a system generated random number. The system displays a 10-digit number in the `Password` field. Take note of this number, your user will need it at home to access the server running Communication Manager.
5. Enter `Doe, John` and click **OK**.

   This is the last name and first name of the user. The system returns you to the Password Manager screen.
6. Select **CommLink:Select Cards**.

   A screen containing a list of cards (for example, Card A, Card B, and so on) appears. Each card corresponds to a port on your Avaya S8XXX Server.
7. Select **Card A** and click **OK**.
8. Select **CommLink:Upload Password**.

   The error message screen appears with the message “`Administrator password not loaded`".
9. Click **OK**.
10. Enter `123456` and click **OK**.
11. Select **CommLink:Upload Password**.
12. When upload is complete, click `OK`.
13. Select **File:Save As**.
14. Enter `doe.fil` in the **File** field and click **OK** to save your changes.

Call Forwarding setup for telecommuting

Communication Manager allows you to change your call forwarding from any on-site or off-site location.

Setting up Call Forwarding for telecommuting example

About this task

In our example, we assign the feature access codes and class of service to set up call forwarding. This allows your users to forward their calls to another extension. For information about the screens referred in this topic, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Procedure

1. Enter `change feature-access-codes`.
2. Set a 2-digit access code for the following fields.
   a. Enter `Extended Call Fwd Activate Busy D/A` field.
   b. Enter `*7` in the **Extended Call Fwd Activate All** field.
   c. Enter `*6` in the **Extended Call Fwd Activate Deactivation** field.

   This sets the access codes for these features. The Command prompt appears.
3. Enter `change cos`.
4. Set the following fields to`y`.
   - **Extended Forwarding All**
   - **Extended Forwarding B/DA**

   This allows you to change the forwarding of all your calls from an off-site location.
5. Set the **Restrict Call Fwd-Off Net** field to `n`.

   See *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205*,* for a description of the Call Forwarding feature.

   See *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for a description of the Tenant Partitioning feature.

   See Telecommuting settings changes for information on how to change call forwarding.

Interactions for Call Forwarding

- Bridged Appearance

  When the pound key (#) is pressed from a bridged appearance immediately following any of this feature's four feature access codes (FACs), the system assumes that the currently active bridged extension will be administered. The station security code of the currently active bridged extension must be entered after the initial # to successfully complete the command sequence.

  If the station has only bridged appearances, the station's extension must be dialed after the FAC to successfully complete the command sequence, since the station's extension is not associated with any appearances.

- Distributed Communications System

  Assign a different telecommuting access extension for each server running Communication Manager. You can use Extended User Administration of Redirected Calls from any of the DCS nodes, but you must dial the extension of the node on which your station is defined before dialing the FAC.

- Tenant Partitioning

  The telecommuting access extension is always automatically assigned to Tenant Partition 1, so it can be accessed by all tenants.

  The tenant number of the extension being administered must be accessible by the tenant number from which the Extended User Administration of Redirected Calls FAC is dialed or the request is denied. If the FAC is dialed on site, the tenant number of the station or attendant must have access to the tenant number of the extension administered. If the FAC is dialed off site, the tenant number of the incoming trunk must have access to the tenant number of the extension administered.

Coverage options assignment for telecommuting

Communication Manager allows you to assign two previously administered coverage paths and/or time of day coverage tables on the Station screen. This allow telecommuters to alternate between the two coverage paths and/or time of day coverage tables administered to better control how their telephone calls are handled.

For information about creating a coverage path, see Creating coverage paths.

For information about creating a time of day coverage table, see Assigning a coverage path to users.

See Telecommuting settings changes for information on how to alternate your coverage path option.

Related topics:
Creating coverage paths on page 232
Assigning a coverage path to users on page 233
Telecommuting settings changes on page 422

Assigning coverage for telecommuting example

About this task

In our example, we assign two coverage options so a user can choose from either option to control how their calls are handled. For information about the screens referred in this topic, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Procedure

1. Enter `change feature-access-codes`.
2. Enter `#9` in the **Change Coverage Access Code** field.
3. Enter `change cor 1`.
4. In the **Can Change Coverage** field, enter `y` and select `Enter` to save your changes.
5. Enter `change station 1234`.

   This is the station extension you configured for telecommuting. The Station screen appears.
6. Complete the following fields:
   a. Enter `2` in the **Coverage Path 1** field.
   b. Enter `8` in the **Coverage Path 2** field.

   See Coverage Path in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for information about and field descriptions on the Coverage Path screen.

   See *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205*,* for a description of the Call Coverage feature.

   See *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for information about the Extended User Administration of Redirected Calls feature.

Home Equipment Installation

Communication Manager allows you to install equipment in your home so that you can utilize system facilities from off-site.

See Communication Manager Configuration for Telecommuting for step-by-step instructions on how to configure your office equipment.

See Telecommuting settings changes for step-by-step instructions on how to use your home station.

Preparing to install home equipment

About this task

You can also set up telecommuting with an IP (internet protocol) telephone or IP Softphone. For example, see Adding an H.323 Softphone for more information.

Procedure

1. For DCP telecommuting, verify that you have the following equipment:
    - Communication Manager extender remote module
    - DCP sets (office and home must match)
2. Configure a feature access code for associating your home number to your office number.

    For information about configuring an associate feature access code, see Personal Station Access setup.

Installing home equipment example

Procedure

1. Plug the telephone cord into the slot labeled line on the back of the module and into the wall jack.
2. Plug the telephone cord into the slot labeled port on the back of the module and into the slot labeled line on the telephone.
3. Plug the power cord into slot labeled power on the back of the module and the wall socket.

The telephone display `Go Online` appears.

4. Press `3 (Nxt).`

   The telephone display `Set Phone Number` appears.

5. Press `2 (OK)` to set the telephone number.

6. Enter `5551234` and press `Drop`.

   This is the assigned analog telephone number. In some areas, you might need to include your area code (for example, 3035551234). The telephone display `Set Phone Number` appears.

7. Press `1(Prv).`

   This returns you to the `Go Online` telephone display.

8. Press `2 (OK).`

   The module dials the number. When the modules connect, the telephone displays `Enter Password`.

9. Enter `0123456789` and press `Drop`.

Associating your office telephone number to the home station example

Procedure

1. On your home station, enter `#4`.

   This is the associate feature access code.

2. Enter `4321` and press `#`.

   This is your extension number.

3. Enter `1996` press `#` .

   This is your password.

Disassociating your home station

Procedure

Press `Hold` four times.

Remote Access setup

Remote Access provides you with access to the system and its features from the public network. This allows you to make business calls from home or use Recorded Telephone Dictation Access to dictate a letter. If authorized, you can also access system features from any on-site extension.

With Remote Access you can dial into the system using Direct Inward Dialing (DID), Central Office (CO), Foreign Exchange (FX), or 800 Service trunks. When a call comes in on a trunk group dedicated to Remote Access, the system routes the call to the Remote Access extension you have assigned. If DID is provided and the Remote Access extension is within the range of numbers that can be accessed by DID, Remote Access is accessed through DID.

Barrier codes provide your system security and define calling privileges through the administered COR. You can administer up to 10 barrier codes, each with a different COR and COS. Barrier codes can be from 4 to 7 digits, *but all codes must be the same length*. You can also require that users enter an authorization code to use this feature. Both barrier codes and authorization codes are described under Authorization Codes setup.

See *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for a description of the Remote Access feature.

Security alert:

Avaya has designed the Remote Access feature incorporated in this product that, when properly administered by the customer, will enable the customer to minimize the ability of unauthorized persons to gain access to the network. It is the customer's responsibility to take the appropriate steps to properly implement the features, evaluate and administer the various restriction levels, protect access codes and distribute them only to individuals who have been advised of the sensitive nature of the access information. Each authorized user should be instructed concerning the proper use and handling of access codes.

In rare instances, unauthorized individuals make connections to the telecommunications network through use of remote access features. In such an event, applicable tariffs require that the customer pay all network charges for traffic. Avaya cannot be responsible for such charges, and will not make any allowance or give any credit for charges that result from unauthorized access.

If you do not intend to use Remote Access now or in the future, you can permanently disable the feature. If you do decide to permanently disable the feature, it will require Avaya Services intervention to activate the feature again.

Preparing to setup Remote Access

Procedure

1. Configure the **Incoming Destination** and **Night Service** fields on the CO Trunk screen.

   For information about configuring a CO trunk, see CO, FX, or WATS trunk group administration.

2. Verify that the **Authorization Codes** field on the System Parameters Customer-Options (Optional Features) screen is set to y.

3. Verify that the **SVN Authorization Code Violation Notification Enabled** field on the Security-Related System Parameters screen is set to y.

Setting up remote access example

About this task

In our example, we set up a remote access extension with maximum security. This assists you in blocking unauthorized people from gaining access to your network.

Procedure

1. Enter `change remote-access` and select `Enter`.

2. On the Remote Access screen enter `1234` in the **Remote Access Extension** field.

   This is the extension specified in the **Incoming Destination** field on the CO Trunk screen.

3. Enter `7` in the **Barrier Code Length** field.

   This is the number of digits your barrier code must be when entered.

4. Enter `y` in the **Authorization Code Required** field.

   This means you must also enter an authorization code when you access the system's Remote Access facilities. For information about setting up access codes, see Authorization Codes setup.

5. Enter`y` in the **Remote Access Dial Tone** field.

   This means you hear dial tone as a prompt to enter your authorization code.

6. Enter `1234567` in the **Barrier Code** field.

   This is the 7-digit barrier code you must enter to access the system's Remote Access facilities.

7. Type `1` in the **COR** field.

   This is the class of restriction (COR) number associated with the barrier code that defines the call restriction features.

8. Enter `1` in the `TN` field.

   This is the Tenant Partition (TN) number.

9. Enter `1` in the **COS** field.

   This is the class of service (COS) number associated with the barrier code that defines access permissions for Call Processing features.

10. Type the expiration date in the **Expiration Date** field.

    This is the date the barrier code expires. A warning message is displayed on the system copyright screen seven days before the expiration date. The system administrator can modify the expiration date to extend the time interval, if necessary.

11. Enter `y` in the **Disable Following A Security Violation** field.

    This disables the remote access feature following detection of a remote access security violation.

12. Select `Enter` to save your work.

Disabling remote access permanently

Procedure

1. Enter `change remote-access`.

2. Enter `y` in the **Permanently Disable** field.

   If you permanently disable this feature, it requires Avaya Services intervention to reactivate the feature. There is a charge for reactivation of this feature.

3. Select `Enter` to save your work.

   ⚠ **Caution:**

   Your attempt to disable the Remote Access feature will be lost if the server running Communication Manager is rebooted without saving translations. Therefore, execute a **`save translation`** command after permanently disabling the Remote Access feature.

Secure Shell remote login

You can log in remotely to the following platforms using Secure Shell (SSH), a secure protocol:

- G250, G350, G430, G450, and G700 Media Gateways
- S8300D, S8510, and S8800 Servers Linux command line
- Communication Manager System Administration Terminal (SAT) interface on an Avaya S8XXX Server using port 5022.

The SSH capability provides a highly secure method for remote access. The capability also allows a system administrator to disable Telnet when it is not needed, making for a more secure system.

Note:

The client device for remote login must also be enabled and configured for SSH. Refer to your client P.C. documentation for instructions on the proper commands for SSH.

Telecommuting settings changes

Communication Manager allows you to associate and disassociate PSA, change the coverage path for your station, change the extension to which you forward your calls, and change your personal station's security code.

Changing Telecommuting settings

Procedure

1. Configure PSA.

   For information about configuring PSA, see Personal Station Access setup.
2. Assign two coverage options for your system.

   For information on how to assign coverage options, see Coverage options assignment for telecommuting.
3. Configure call forwarding for your system.

   For information about configuring call forwarding, see Call Forwarding setup for telecommuting.
4. Configure security codes for a station.

For information about configuring personal station security codes, see Assigning an Extender Password example.

Associating PSA example

About this task

In this example, we associate PSA (preferences and permissions) assigned to your station with another compatible terminal.

Procedure

1. Dial **#4**.

   This is the associate PSA feature access code. You hear dial tone.
2. Enter**1234** and press # .

   This is your extension.
3. Enter **4321** and press #.

   This is your Station Security Code. You hear a confirmation tone.

Disassociating PSA example

About this task

In our example, we disassociate PSA from the station you are using.

Procedure

Dial #3.

This is the disassociate PSA feature access code. You are no longer PSA associated to this station.

Changing a coverage option example

About this task

In this example, we change the coverage option from path 1 to path 2 from a remote location.

Procedure

1. Dial `1234`.

   This is the extension you configured for telecommuting. You hear dial tone.
2. Dial `#9` and press `#`.

   This is the feature access code you set for changing a coverage path. You hear dial tone.
3. Dial `4321` and press `#`.

   This is the extension for which you want to change the coverage path.
4. Dial `87654321`.

   Press `#`.

   This is the extension security code.
5. Dial `2`.

   This is the new coverage path. You hear confirmation tone.

Changing call forwarding example

About this task

In this example, we change call forwarding to extension 1235.

Procedure

1. Dial `1234`.

   This is the extension you configured for telecommuting.
2. Dial **`#8`** and press `#` .

   This is the feature access code you set for activating extended call forward. You hear dial tone.
3. Dial `4321` and press `#` .

   This is the extension from which you want to forward calls.
4. Dial `87654321` and press `#` .

   This is the extension security code. You hear dial tone.
5. Dial `1235`.

   This is the extension to which you want to forward calls. You hear the confirmation tone.

Changing your personal station security codes example

About this task

In this example, we change the security code for extension 1235 from 98765432 to 12345678.

Procedure

1. Dial `#5`.

   This is the feature access code you set for changing your security code. You hear dial tone.

2. Dial `1235` and press `#` .

   This is the extension for which you want to change the security code.

3. Dial `98765432` and press `#` .

   This is the current security code for the extension. You hear dial tone.

4. Dial `12345678` and press `#` .

   This is the new security code. Security codes can be 3-8 digits long.

5. Dial `12345678`.

   Press **#**.

   This is to confirm your new security code. You hear the confirmation tone.

   Note:

   If you cannot change your security code, Manager 1 can clear the problem using the **`Clear Audit Summary`** command.

Interrupting the command sequence for personal station security codes

Procedure

1. To interrupt the command sequence before step 3, choose one of these options:

   - Hang up or press the disconnect or recall button before hearing intercept tone in step 3.

     The system does not log an invalid attempt. You must restart the process at step 1.

   - Type `*` before the second # in step 3.

You must begin the change sequence at the point of entering your extension in step 2. (You should not enter the FAC again.)

- Type * after the FAC has been entered and before the final #.

  You must restart the process at step 1.

2. To interrupt the command sequence after step 3, type * in steps 4 or 5, you must begin the change sequence at the point of entering the new station security code (SSC) in step 4.

   If you hear intercept tone in any step, the command sequence has been invalidated for some reason and you must restart the process at step 1.

   If you hear intercept tone after step 3, the system logs an invalid attempt via the Security Violations Notification (SVN) feature. This is true even if you attempt to interrupt the change sequence with an asterisk.

Chapter 14: Enhancing System Security

Basic Security recommendations

Keep your system secure

The following is a partial list you can use to help secure your system. It is not intended as a comprehensive security checklist. See the *Avaya Toll Fraud and Security Handbook*, 555-025-600, for more information about these and other security-related features.

1. Secure the system administration and maintenance ports and/or logins on Communication Manager using the Access Security Gateway. This optional password authentication interface program is provided to customers with maintenance contracts.
2. Activate Security Violations Notification to report unsuccessful attempts to access the system. Security Violations Notification lets you automatically disable a valid login ID following a security violation involving that login ID and disable remote access following a security violation involving a barrier code or authorization code.
3. Secure trunks using Automatic Route Selection (ARS), Class of Restriction (COR), Facility Restriction Levels (FRLs) and Alternate Facility Restriction Levels (AFRLs), Authorization Codes, Automatic Circuit Assurance (ACA), and Forced Entry of Account Codes (see Call Detail Recording in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information).
4. You can log in remotely using Secure Shell (SSH) as a secure protocol. The SSH capability provides a highly secure method for remote access. The capability also allows a system administrator to disable Telnet when it is not needed, making for a more secure system.
5. Activate Enhanced Call Transfer for your voice messaging system, if available. This limits transfers to valid extensions, but you also need to restrict transfers to extensions that might offer dial tone to the caller, such as screen extensions.

Toll Fraud prevention

Preventing toll fraud — top 15 tips to help

Procedure

1. Protect system administration access

   Make sure secure passwords exist for all logins that allow System Administration or Maintenance access to the system. Change the passwords frequently.

   Set logoff notification and forced password aging when administering logins. You must assign passwords for these logins at setup time.

   Establish well-controlled procedures for resetting passwords.

2. Prevent voice mail system transfer to dial tone

   Activate “secure transfer” features in voice mail systems.

   Place appropriate restrictions on voice mail access/egress ports.

   Limit the number of invalid attempts to access a voice mail to five or less.

3. Deny unauthorized users direct inward system access (screen)

   If you are not using the Remote Access features, deactivate or disable them.

   If you are using Remote Access, require the use of barrier codes and/or authorization codes set for maximum length. Change the codes frequently.

   It is your responsibility to keep your own records regarding who is allowed to use which authorization code.

4. Place protection on systems that prompt callers to input digits

   Prevent callers from dialing unintended digit combinations at prompts.

   Restrict auto attendants and call vectors from allowing access to dial tone.

5. Use system software to intelligently control call routing

   Create Automatic Route Selection or World Class Routing patterns to control how each call is to be handled.

   Use “Time of Day” routing capabilities to limit facilities available on nights and weekends.

   Deny all end-points the ability to directly access outgoing trunks.

6. Block access to international calling capability

   When international access is required, establish permission groups.

   Limit access to only the specific destinations required for business.

7. Protect access to information stored as voice

   Password restrict access to voice mail mailboxes.

   Use non-trivial passwords and change passwords regularly.

8. Provide physical security for telecommunications assets

   Restrict unauthorized access to equipment rooms and wire connection closets.

   Protect system documentation and reports data from being compromised.

9. Monitor traffic and system activity for abnormal patterns

   Activate features that “turn off” access in response to unauthorized access attempts.

   Use Traffic and Call Detail reports to monitor call activity levels.

10. Educate system users to recognize toll fraud activity and react appropriately

    From safely using calling cards to securing voice mailbox password, train your users on how to protect themselves from inadvertent compromises to the system’s security.

11. Monitor access to the dial-up maintenance port.

    Change the access password regularly and issue it only to authorized personnel. Consider activating Access Security Gateway. See Access Security Gateway in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205 for more information.

12. Create a system-management policy concerning employee turnover and include these actions:

    a. Delete any unused voice mailboxes in the voice mail system.
    b. Immediately delete any voice mailboxes belonging to a terminated employee.
    c. Immediately remove the authorization code if a terminated employee had screen calling privileges and a personal authorization code.
    d. Immediately change barrier codes and/or authorization codes shared by a terminated employee.

       Notify the remaining users of the change.
    e. Remove a terminated employee’s login ID if they had access to the system administration interface.

       Change any associated passwords immediately.

13. Back up system files regularly to ensure a timely recovery.

    Schedule regular, off-site backups.

14. Callers misrepresenting themselves as the “telephone company,” “AT&T,” “RBOCS,” or even known employees within your company might claim to be testing the lines and ask to be transferred to “900,” “90,” or ask the attendant to do “start 9 release.” This transfer reaches an outside operator, allowing the unauthorized caller to place a long distance or international call.

Instruct your users to never transfer these calls. Do not assume, that if “trunk to trunk transfer” is blocked, this cannot happen.

Hackers run random generator PC programs to detect dial tone. Then they revisit those lines to break barrier codes and/or authorization codes to make fraudulent calls or resell their services. They do this using your telephone lines to incur the cost of the call. Frequently these call/sell operations are conducted at public pay phones located in subways, shopping malls, or airport locations. See Security Violations Notification setup to prevent this happening to your company.

Enforcing physical security

About this task

Physical security is your responsibility. Implement the following safeguards as an added layer of security:

Procedure

1. Unplug and secure attendant console handsets when the attendant position is not in use.
2. Lock wiring closets and server rooms.
3. Keep a log book register of technicians and visitors.
4. Shred all Communication Manager information or directories you discard.
5. Always demand verification of a technician or visitor by asking for a valid I.D. badge.
6. Keep any reports that might reveal trunk access codes, screen barrier codes, authorization codes, or password information secure.
7. Keep the attendant console and supporting documentation in an office that is secured with a changeable combination lock.

   Provide the combination only to those individuals who need to enter the office.
8. Keep any documentation pertaining to Communication Manager operation secure.
9. Label all backup tapes or flash cards with correct dates to avoid using an outdated one when restoring data.

   Be sure that all backup media have the correct generic software load.

Checking system security

About this task

Here's some of the steps required for indemnification. Use these to analyze your system security.

Procedure

1. Remove all default factory logins of **cust**, **rcust**, **browse**, **nms**, and **bcms** and assign unique logins with 7-character alphanumeric passwords and a 90-day password aging.

   Use the `list logins` command to find out what logins are there.

2. If you do not use Remote Access, be sure to disable it permanently.

   Tip:

   You can use the `display remote-access` command to check the status of your remote access.

   To disable Remote Access, on the Remote Access screen, in the **Permanently Disable** field, enter `y`.

   Note:

   Avaya recommends that you permanently disable Remote Access using the `change remote-access` command. If you do permanently disable Remote Access, the code is removed from the software. Avaya charges a fee to restore the Remote Access feature.

3. If you use Remote Access, but only for internal calls, change announcements or remote service observing.

   a. Use a 7-digit barrier code.

   b. Assign a unique COR to the 7-digit barrier code.

      The unique COR must be administered where the **FRL** is `0`, the **Calling Party Restriction** field is `outward`, and the **Calling Permissions** field is `n` on all unique Trunk Group COR.

   c. Assign **Security Violation Notification Remote** to `10` attempts in `2` minutes.

   d. Set the aging cycle to `90` days with `100` call limit per barrier code.

4. If you use Remote Access to process calls off-net or in any way access the public network:

   a. Use a 7-digit barrier code.

   b. Assign a unique COR to the barrier code.

c. Restrict the COR assigned to each barrier code by FRL level to only the required calling areas to conduct business.

d. Set the aging cycle to `90` days with `100` call limit per barrier code.

e. Suppress dial tone where applicable.

f. Administer Authorization Codes.

g. Use a minimum of 11 digits (combination of barrier codes and authorization codes).

h. Assign **Security Violation Notification Remote** to 10 attempts in 2 minutes.

5. If you use vectors:

a. Assign all Vector Directory Numbers (VDN) a unique COR.

See *Avaya Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568, and *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780*,* for more information.

Note:

The COR associated with the VDN dictates the calling privileges of the VDN/vector. High susceptibility to toll fraud exists on vectors that have “collect digits” steps. When a vector collects digits, it processes those digits back to Communication Manager and if the COR of the VDN allows it to complete the call off-net, it will do so. For example, the announcement “If you know your party’s 4-digit extension number, enter it now” results in 4 digits being collected in step 6. If you input “90##” or “900#”, the 4 digits are analyzed and if “9” points towards ARS and “0” or “00” is assigned in the ARS Analysis Tables and the VDN COR allows it, the call routes out of the server to an outside local exchange or long distance operator. The operator then connects the call to the requested number.

b. If vectors associated with the VDN do not require routing the call off-net or via AAR, assign a unique COR where the **FRL** is `0`, the **Calling Party Restriction** field is `outward`, the **Calling Permissions** field is `n` on all unique Trunk Group COR.

c. If the vector has a “route-to” step that routes the call to a remote server via AAR, assign a unique COR with a unique ARS/AAR Partition Group, the lowest FRL to complete an AAR call, and `n` on all unique COR assigned to your public network trunking facilities on the Calling Permissions.

Assign the appropriate AAR route patterns on the AAR Partition Group using the **`change aar analysis partition x 2`** command.

Tip:

You can use the **`display aar analysis print`** command to print a copy of your Automatic Alternate Routing (AAR) setup before making any changes. You can use the printout to correct any mistakes.

d. If the vector has a “route-to” step that routes the call to off-net, assign a unique COR with a unique ARS/AAR Partition Group, the lowest FRL to complete an

ARS call, and `n` on all unique COR assigned to your public network trunking facilities on the Calling Permissions.

Assign the appropriate complete dial string in the "route-to" step of the vector the unique ARS Partition Group using the **`change ars analysis partition x 2`** command.

6. On the Feature Access Code (FAC) screen, **Facility Test Calls Access Code**, the **Data Origination Access Code**, and the **Data Privacy Access Code** fields, change from the default or remove them.

   For information about the Feature Access Code (FAC) screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

   Note:

   These codes, when dialed, return system dial tone or direct access to outgoing trunking facilities. Transfers to these codes can take place via an unsecured vector with "collect digits" steps or an unsecured voice mail system.

7. Restrict Call Forwarding Off Net on every class of service.

   See *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information on Class of Service.

   Note:

   You cannot administer loop-start trunks if Call Forwarding Off Net is required.

8. If loop start trunks are administered on Communication Manager and cannot be changed by the Local Exchange Company, block all class of service from forwarding calls off-net.

   In the Class of Service screen, **Restriction Call Fwd-Off Net** field, set to `y` for the 16 (0-15) COS numbers.

   See *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information on Class of Service.

   Note:

   If a station is call forwarded off-net and an incoming call to the extension establishes using a loop-start trunk, incorrect disconnect supervision can occur at the Local Exchange Central Office when the call terminates. This gives the caller recall or transfer dial tone to establish a fraudulent call.

9. Administer Call Detail Recording on all trunk groups to record both incoming and outgoing calls.

   See Call information collection for more information.

10. On the Route Pattern screen, be careful assigning route patterns with an **FRL** of `0`; these allow access to outgoing trunking facilities.

    Avaya recommends assigning routes with an **FRL** of `1` or higher.

Note:

An exception might be assigning a route pattern with an **FRL** of `0` to be used for 911 calls so even restricted users can dial this in emergencies.

Tip:

You can use the **`list route-pattern print`** command to print a copy of your FRLs and check their status.

11. On all Trunk Group screens, set the **Dial Access** field to `n`.

    If set to `y`, it allows users to dial Trunk Access Codes, thus bypassing all the ARS call screening functions.

    See the Trunk Group section of *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information.

12. On the AAR and ARS Digit Analysis Table, set all dial strings not required to conduct business to `den` (deny).

    For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

13. If you require international calling, on the AAR and ARS Digit Analysis Table, use only the 011+ country codes/city codes or specific dial strings.

14. Assign all trunk groups or same trunk group types a unique Class of Restriction.

    If the trunk group does not require networking through Communication Manager, administer the Class of Restriction of the trunk group where the **FRL** is `0`, the **Calling Party Restriction** field is `outward`, and all unique Class of Restriction assigned to your outgoing trunk groups are `n`. See Class of Restriction in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information.

    Tip:

    You can use the **`list trunk-group print`** command to have a printout of all your trunks groups. Then, you can use the **`display trunk-group x`** command (where **`x`** is the trunk group) to check the COR of each trunk group.

15. For your Communication Manager Messaging, on the System Appearance screen, set:

    - the **Enhanced Call Transfer** field to `y`.
    - the **Transfer Type** field to `enhanced`. If set to `basic`, set the **Transfer Restriction** field to `subscribers`. See Feature-Related System Parameters in *Avaya Aura™ Communication Manager* Screen Reference, 03-602878, for more information.

      Note:

      The COR of the voice mail ports dictates the calling restrictions of the voice mail. If the above settings are not administered correctly, the possibility exists to complete a transfer to trunk access codes or ARS/AAR feature codes for fraudulent purposes. Never assign mailboxes that begin with the digits or trunk access codes of ARS/AAR feature access codes. Require your users to use a mailbox password length greater than the amount of digits in the extension number.

16. Avaya recommends you administer the following on all voice mail ports:

    - Assign all voice mail ports a unique COR. See Class of Restriction in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information.
    - If you are not using outcalling, fax attendant, or networking, administer the unique COR where the **FRL** is `0`, the **Calling Party Restriction** field is `outward`, and all unique trunk group COR on the Calling Permissions are `n`. See Class of Restriction in *Avaya Aura™ Communication Manager* Screen Reference, 03-602878, for more information.

Note:

Avaya recommends you administer as many layers of security as possible. You can implement Step 9 and Step 16 as a double layer of security. In the event that the voice mail system becomes unsecured or compromised for any reason, the layer of security on Communication Manager takes over, and vice versa.

17. Administer all fax machines, modems, and answering machines analog voice ports as follows:

    - Set the **Switchhook Flash** field to `n`.
    - Set the **Distinctive Audible Alert** field to `n`. See Station in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information.

18. Install a Call Accounting System to maintain call records.

    In the CDR System Parameters screen, **Record Outgoing Calls Only** field, set to `y`. See CDR System Parameters in *Avaya Aura™ Communication Manager* Screen Reference, 03-602878, for more information.

19. Call Accounting Systems produce reports of call records.

    It detects telephones that are being hacked by recording the extension number, date and time of the call, and what digits were dialed.

User Profiles and Logins administration

Authentication, Authorization and Accounting (AAA) Services allows you to store and maintain administrator account (login) information on a central server. Login authentication and access authorization is administered on the central server.

For details on administering user profiles and logins, see AAA Services in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, and *Maintenance Commands for Avaya Aura™ Communication Manager*, 03-300431.

Access Security Gateway (ASG)

For more information on ASG, see Access Security Gateway in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

For more information on SVN, see Security Violations Notification in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Busy Verify toll fraud detection

This section shows you how to use Busy Verify (also known as Busy Verification) to help find fraud problems.

When you suspect toll fraud, you can interrupt the call on a specified trunk group or extension number and monitor the call in progress. Callers will hear a long tone to indicate the call is being monitored.

! Security alert:

Listening to someone else's calls might be subject to federal, state, or local laws, rules, or regulations. It might require the consent of one or both of the parties on the call. Familiarize yourself with all applicable laws, rules, and regulations and comply with them when you use this feature.

Preparing to use busy verify for toll fraud detection

Procedure

On the Trunk Group screen - page 1, verify the **Dial Access** field is `y`.

If it is not, contact your Avaya technical support representative.

Using busy verify for toll fraud detection example

Procedure

1. Enter `change station` **`xxxx`**, where **`xxxx`** is the station to be assigned the busy verify button.

   Press `Enter`.

   The system displays the Station screen. For this example, enter extension `1014`. Press **Next Page** until you see the **Site Data** fields.
2. In the **BUTTON ASSIGNMENTS** area, enter `verify` and select `Enter` to save your changes.
3. To activate the feature, press the `Verify` button on the telephone and then enter the `Trunk Access Code` and member number to be monitored.

Authorization Codes setup

Authorization codes provide the means for extending control of system users' calling privileges. They extend calling-privilege control and provide an extra level of security for remote-access callers.

Note:

To maintain system security, Avaya recommends you use authorization codes.

See the *Avaya Toll Fraud and Security Handbook*, 555-025-600 for more information.

Preparing to setup Authorization Codes

Procedure

On the screen, verify the **Authorization Codes** field is `y`.

If not, contact your Avaya representative. This field turns on the feature and permits you to selectively specify levels of calling privileges that override in-place restrictions.

Setting Up Authorization Codes example

Procedure

1. Enter **`change system-parameters features`** and press `Enter`.
2. Click **Next** until you find the **Authorization Code Enabled** field.
3. In the **Authorization Code Enabled** field, enter`y`.

   This enables the Authorization Codes feature on a system-wide basis.
4. In the **Authorization Code Length** field, enter `7`.

   This defines the length of the Authorization Codes your users need to enter. To maximize the security of your system, Avaya recommends you make each authorization code the maximum length allowed by the system.
5. In the **Authorization Code Cancellation Symbol** field, leave the default of `#`.

   This is the symbol a caller must dial to cancel the 10-second wait period during which your user can enter an authorization code.
6. In the **Attendant Time Out Flag** field, leave the default of `n`.

   This means a call is not to be routed to the attendant if a caller does not dial an authorization code within 10 seconds or dials an invalid authorization code.
7. In the **Display Authorization Code** field, enter `n`.

   This prevents the authorization code from displaying on telephone sets thus maximizing your security.
8. Select `Enter` to save your changes.
9. Enter `change authorization-code` **`nnnn`**, where **`nnnn`** is the authorization code, and press `Enter`.
10. In the **AC** field, enter the authorization code your users must dial.

In this example, type `4285193`. The number of digits entered must agree with the number assigned in the Feature-Related System Parameters screen, **Authorization Code Length** field.

> **Note:**
>
> Remember, all authorization codes used in the system must be the same length.

11. In the **COR** field, enter the desired Class of Restriction number from 0 through 95.

    In our example, type `1`.

12. Enter `change trunk-group` **`n`**, where **`n`** is the assigned trunk group number, and press `Enter`.

13. In the **Auth Code** field, enter `y` to require callers to enter an authorization code in order to tandem a call through an AAR or ARS route pattern.

    The code will be required even if the facility restriction level of the incoming trunk group is normally sufficient to send the call out over the route pattern.

14. Select `Enter` to save your changes.

Related information for Authorization Codes

See Class of Restriction in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information on setting up dialing out restrictions.

See *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504, for more information on using trunk access codes.

See Facility Restriction Levels and Traveling Class Marks *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205 and Route Pattern in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information on assigning Facility Restriction Levels.

See Call Detail Recording in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, and Station in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information on using Call Detail Recording (CDR) on station telephones.

See Class of Restriction and Station in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information on using Class of Restriction (COR) on station telephones.

See Remote Access in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205 for more information on allowing authorized callers to access the system from remote locations.

See Barrier Codes in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205 on page 1341, for information on barrier codes.

See AAA Services in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, and *Maintenance Commands for Avaya Aura™ Communication Manager*, 03-300431 for details on administering user profiles and logins.

Security Violations Notification setup

This section shows you how to use Security Violations Notification (SVN) to set security-related parameters and to receive notification when established limits are exceeded. You can run reports related to invalid access attempts. You also can disable a login ID or remote access authorization that is associated with a security violation.

When a security violation has occurred, there are steps that you can take to be sure that this same attempt is not successful in the future. See the *Avaya Toll Fraud and Security Handbook*, 555-025-600, for more information.

Setting up Security Violations Notification example

Procedure

1. Enter `change system-parameters security` and press `Enter` to open the Security-Related System Parameters screen.
2. Enter `y` in the **SVN Login Violation Notification Enabled** field.

   This sets Security Violations Notification login violation notification.

   Note:

   If you are not using Security Violation Notification for logins, enter`n` in the **SVN Login Violation Notification Enabled** field and go to Step 6.
3. In the **Originating Extension** field, enter `3040`.

   This becomes the telephone extension for the purpose of originating and identifying SVN referral calls for login security violations.
4. In the **Referral Destination** field, enter `attd` to send all calls to the attendant.

   This is the telephone extension that receives the referral call when a security violation occurs.
5. Select `Enter` to save your changes.

   Note:

   If you are not using Remote Access, go to Step 9.

6. (Optional) Type **`change remote-access`** and press `Enter`.
7. (Optional) In the **Disable Following A Security Violation** field, type `y`.

   This disables Remote Access following detection of a remote access security violation.
8. (Optional) Press `Enter` to save your changes.
9. Type **`change station xxxx`**, where **`xxxx`** is the station to be assigned the notification halt button and press `Enter`.
10. In the BUTTON ASSIGNMENTS section, type one of the following:
    - **`asvn-halt`** — The Authorization Code Security Violation Notification call is activated when an authorization code security violation is detected. This applies only if you are using authorization codes.
    - **`lsvn-halt`** — The Login Security Violation Notification call is activated a referral call when a login security violation is detected.
    - **`rsvn-halt`** — The Remote Access Barrier Code Security Violation Notification call is activated as a call referral. This applies only if you are using Remote Access barrier codes.
    - **`ssvn-halt`** — The Station Code Security Violation Notification call is activated when a station code security violation is detected. This applies only if you are using station codes.

    Note:

    Any of the above 4 security violations will cause the system to place a notification call to the designated telephone. The call continues to ring until answered. To stop notification of any further violations, press the button associated with the type of violation.
11. Press `Enter` to save your changes.

Enhanced security logging

Enhanced security logging increases the granularity of logging of user activity, and allows you to specify an external server or Linux syslog to which to send a copy of system logs. Enhanced security logging consolidates several existing Communication Manager log files, and routes copies of the files to an industry standard external log server or the internal Linux syslog.

SAT activities are logged according to a logging level set by the administrator using the SAT Logging Levels screen.

On the Integrated Management Maintenance Web Pages, use the Syslog Server web screen to enable or disable the ability to send logs to an external server, and to specify the logs to be sent.

Station lock

Detailed description of Station Lock

With the Station Lock feature, users can lock the telephone to prevent others from placing outgoing calls from the telephone.

A user with an analog telephone uses a Feature Access Code (FAC) to lock the telephone. A user with a digital telephone can use a FAC or a feature button to lock the telephone. Station Lock:

- Blocks unauthorized outgoing calls
- Allows outgoing emergency calls
- Allows incoming calls

The feature button lights when the user presses the button to activate Station Lock. Then, when a user attempts to place an outgoing call, the system generates a special dial tone to indicate that the Station Lock feature is active.

Only H.323 or DCP phones support the station lock functionality of Communication Manager. SIP phones do not support the functionality.

If a digital or an IP station has a Station Lock button but activates the feature with the FAC, the LED for the button lights and special dial tone is provided.

If a digital or an IP station does not have a Station Lock button and activates the feature with the FAC, a special dial tone is provided.

Avaya recommends that a user of a digital telephone use a **Station Lock** button, instead of a FAC, to activate Station Lock.

Any user who knows the system-wide FAC for Station Lock, and the Station Security Code (SSC) of a specific telephone, can lock or unlock the telephone.

A user can also lock or unlock a telephone from a remote location.

The attendant console can lock or unlock other telephones. The attendant console cannot be locked.

Preparing to set up Station Lock

Procedure

Be sure the **Station Lock COR** field on the Class of Restriction screen has the COR that the user is using to define the calling restrictions.

Setting up Station Lock with a Station Lock button example

About this task

We will set Station Lock to allow authorized users to access the system through a particular station (extension 7262).

Procedure

1. Enter `change station 7262`.
2. In the **Security Code** field, enter a security code of up to 8 digits.

   In the **COR** field, leave the default at `1`.
3. In the **BUTTON ASSIGNMENTS** section, type `sta-lock`.
4. Select `Enter` to save your changes.
5. Type **`change cor 1`** and press `Enter`.
6. In the **Calling Party Restriction** field, type `none`.

   This means that no calling party restrictions exist on extension 7262.
7. In the **Station Lock COR** field, type `2`.
8. Select `Enter` to save your changes.
9. Type **`change cor 2`** and press `Enter`.
10. In the **Calling Party Restriction** field, verify it is `outward`.
11. Select `Enter` to save your changes.

    Now when extension 7262 activates Station Lock, calling restrictions are determined by the Station Lock COR, COR 2. Based on the administration of COR 2, extension 7262 is not allowed to call outside the private network. When Station Lock is not active on extension 7262, calling restrictions are determined by the COR administered on the Station screen, COR 1. In this example, when extension 7262 is unlocked, calls outside the private network are allowed.

Setting up Station Lock without a Station Lock button example

About this task

To set Station Lock on an analog, x-mobile, or digital telephone without a Station Lock button (extension 7262 and use a feature access code of 08):

Procedure

1. Enter `change station 7262`.
2. In the **Security Code** field, enter a security code of up to 8 digits.

   In the **COR** field, leave the default at `1`. This means that anyone can call outside on extension 7262.
3. Select `Enter` to save your changes.
4. Enter `change system-parameters features`.
5. In the **Special Dial Tone** field, type `y` for an audible tone indicating the station is locked.
6. Press `Enter` to save your changes.
7. Type **`change feature-access-codes`** and press `Enter`.
8. Move the cursor to the **Station Lock Activation** field.
9. In the **Activation** field, type `*08`.
10. In the **Deactivation** field, enter `#08`.
11. Select**Enter** to save your changes.

    Now when a user activates Station Lock, no one can call outside from extension 7262.

Station Lock by time of day

Beginning with Communication Manager 4.0 or later, you can you can also lock stations using a Time of Day (TOD) schedule.

To engage the TOD station lock/unlock you do not have to dial the station lock/unlock FAC, or use **stn-lock** button push.

When the TOD feature activates the automatic station lock, the station uses the Class of Restriction (COR) assigned to the station lock feature for call processing. The COR used is the same as it is for manual station locks.

The TOD lock/unlock feature does not update displays automatically, because the system would have to scan through all stations to find the ones to update.

The TOD Station Lock feature works as follows:

- If the station is equipped with a display, the display will show "Time of Day Station Locked", if the station invokes a transaction which is denied by the Station Lock COR. Whenever the station is within a TOD Lock interval, the user will hear a special dial tone instead of the normal dial tone, if the special dial tone is administered.
- For analog stations or without a display, the user hears a special dial tone. The special dial tone has to be administered and the user hears it when the station is off hook.

After a station is locked by TOD, it can be unlocked from any other station if the Feature Access Code (FAC) or button is used. You have to also know the Station Security Code, and that the **Manual-unlock allowed?** field on the Time of Day Station Lock Table screen is set to `y`.

Once a station has been unlocked during a TOD lock interval, the station remains unlocked until next station lock interval becomes effective.

If the station was locked by TOD and by Manual Lock, an unlock procedure will unlock the Manual Lock as well as the TOD Lock ("Manual-unlock allowed?" field on the Time of Day Station Lock Table screen is set to `y`).

The TOD feature does not unlock a manually locked station.

Note:

The attendant console cannot be locked by TOD or manual station lock.

Screens for administering Station Lock

Screen name	Purpose	Fields
COR	Administer a Class of Restriction (COR) that allows the user to activate Station Lock with a feature access code (FAC).	**Station Lock COR**
Feature Access Code (FAC)	Assign one FAC for Station Lock activation, and another FAC for Station Lock Deactivation.	**Station Lock Activation** Station Lock Deactivation
Station	Assign the user a COR that allows the user to activate Station Lock with an FAC.	**COR** **Time of Day Lock Table**
	Assign a sta-lock feature button for a user.	Any available button field in the **BUTTON ASSIGNMENTS** area

Screen name	Purpose	Fields
	Assign a Station Security Code (SSC) for a user.	**Security Code**
Time of Day Station Lock Table	Administer station lock by time of day.	**Table Active** **Manual Unlock Allowed** **Time Intervals**
Feature Related System Parameters	Enable special dial tone.	**Special Dial Tone**

Security Violations responses

When a security violation occurs, there are steps that you can take to be sure that this same attempt is not successful in the future.

Enabling remote access

About this task

You may have to enable Remote Access that has been disabled following a security violation, or disabled manually.

Procedure

1. Log in to Communication Manager using a login ID with the correct permissions.
2. Enter `enable remote-access`.

Disabling remote access

About this task

There might be occasions when you have to disable remote access for one of your users because of a security violation.

Procedure

1. Log in to Communication Manager using a login ID with the correct permissions.
2. Enter disable remote-access.

Hot Desking Enhancement

Hot Desking is a generic term for features that enable you to lock and unlock your telephones or to move a fully customized station profile to another compatible telephone. Hot Desking enhances the existing features:

- IP Login/Logoff
- PSA Association/Dissociation
- Station Lock and Time of Day Station Lock

Hot Desking Enhancement (HDE) is limited to the 96xx-series H.323 IP telephones. It does not require any special license to be operational. Parts of the enhancement require firmware changes for the telephones. Only the 96xx-series H.323 IP telephones with the appropriate firmware change support the full range of HDE. The **Hot Desking Enhancement Station Lock** field is available on page 3 of the Feature-Related System Parameters screen.

Hot Desking interaction with PSA

The Hot Desking Enhancement (HDE) feature displays PSA Login information. You can invoke Personal Station Access (PSA) using H.323 IP telephones. If the Hot Desking Enhancement is activated, the telephone displays a text message to inform you how to log in again after PSA logoff. The message is sent to all telephones, including IP (H.323) telephones, if the **Hot Desking Enhancement Station Lock** field on the Feature-Related System Parameters screen is set to y.

Note:

The message is not sent to H.323 telephones on PSA Logoff. If an H.323 telephone is in state PSA Logoff and IP Login is used instead of PSA Login the display text of SA8582 is shown after going off hook/on hook. After dialing the FAC for PSA Login the text disappears.

The message used for displaying the PSA Login information is a non-call associated message, which gets shown at the top of an IP (H.323) telephone.

The **Hot Desking Enhancement Station Lock** field on the System-Parameters Features screen controls the feature.

Station Lock

Use the Station Lock feature to lock a telephone to prevent others from placing outgoing calls from the telephone.

Hot Desking with Station Lock restrictions

Parts of the Hot Desking Enhancement (HDE) feature apply only to telephones with firmware changes, while other parts apply to all telephones. The table here provides an overview. For information on firmware vintage number, contact your Avaya representative.

HDE Feature	96xx H.323 with FW changes	96xx H.323 without FW changes	Other sets with display	Other sets without display
PSA Logoff Display Login Information	X	X	X	–
Station Lock No access to telephone capabilities (Note 1)	X	X	–	–
Station Lock Extension to Cellular blocked (no make, answer and bridge)	X	X	X	X (Note 2)
Station Lock Bridged appearances blocked	X	X	X	X (Note 3)
Station Lock Limited Access to Feature Access Codes and Feature Buttons	X	X	X	X

Note 1: Telephone capabilities are call log, Avaya menu, contact list, USB access and redial button.

Note 2: If the set offers Extension to Cellular.

Note 3: If the set offers bridged appearances.

Chapter 15: Managing Trunks

Tips for working with trunk groups

You'll find detailed procedures for administering specific trunk groups elsewhere in this chapter. However, there's more to working with trunks than just administering trunk groups.

Following a process when working with trunk groups

About this task

Trunking technology is complex. Following a process can prevent mistakes and save you time. Avaya recommends following the process below (some steps might not apply to your situation) to set up new trunks and trunk groups,:

Procedure

1. Install the necessary circuit packs and perform any administration the circuit pack requires.
2. Connect the appropriate ports to your network service provider's trunks.
3. Administer a trunk group to control the operation of the trunks.
4. Assign the ports you're using to the trunk group.
5. For outgoing or 2-way trunks, administer Automatic Route Selection so Communication Manager knows which outgoing calls to route over this trunk group.
6. Test your new trunk group by placing a variety of call using the trunk access code.

   Using the trunk access code, place a variety of calls.

   See Modifying Call Routing for detailed information on Automatic Route Selection.

Service provider coordination for trunk groups

Depending on the type of trunk you want to add, the vendor might be your local telephone company, a long distance provider, or some other service provider. Key settings on

Communication Manager must be identical to the same settings on the provider's equipment for your trunks to work. Clear, frequent communication with your provider is essential — especially since some providers might use different terms and acronyms than Avaya does!

Once you decide that you want to add a new trunk, contact your vendor. The vendor should confirm the type of signal you want and provide you with a circuit identification number for the new trunk. Be sure to record any vendor-specific ID numbers or specifications in case you ever have any problems with this trunk.

Records keeping for trunk groups

In addition to recording vendor-specific information such as ID numbers, you should record the following information about every trunk group you have.

The questions you need to answer	The kind of information you need to get
What type of trunk group is it?	You need to know what kind of trunks these are (central office (CO), foreign exchange (FX), and so on.) and whether they use any special services (such as T1 digital service). You also need to know what kind of signaling the group uses. For example, you might have a CO trunk group with ground-start signaling running on a robbed-bit T1 service.
Which telephone numbers are associated with each trunk group?	For incoming or two-way trunk groups: 1. What number or numbers do outside callers use to call into your server over this group? 2. What is the destination extension to which this trunk group delivers calls? Does it terminate at an attendant or a voice-mail system? For outgoing trunk groups: • What extensions can call out over this trunk group?
Is the service from your network service provider sending digits on incoming calls?	Direct Inward Dial and Direct Inward/Outward Dial trunks send digits to Communication Manager. Tie trunks can send digits, depending on how they're administered. You need to know: • How many digits is your service provider sending? • Are you inserting any digits? What are they? • Are you absorbing any digits? How many? • What range of numbers has your service provider assigned you?

Helpful tips for setting common trunk group fields

The procedures in this section cover the specific fields you must administer when you create each type of trunk group. Here are some tips for working with common fields that are available for most trunk groups.

- Dial Access — Typing `y` in this field allows users to route calls through an outgoing or two-way trunk group by dialing its trunk access code.

  Security alert:

  Calls dialed with a trunk access code over Wide Area Telecommunications Service (WATS) trunks are not validated against the ARS Digit Analysis Table, so users can dial anything they wish. For security, you might want to leave the field set to `n` unless you need dial access to test the trunk group.

- Outgoing Display — Typing `y` in this field allows display telephones to show the name and group number of the trunk group used for an outgoing call. This information might be useful to you when you're trying to diagnose trunking problems.
- Queue Length — Don't create a queue for two-way loop-start trunks, or you might have a problem with glare (the interference that happens when a two-way trunk is seized simultaneously at both ends).
- Trunk Type — Use ground-start signaling for two-way trunks whenever possible: ground-start signaling avoids glare and provides answer supervision from the far end. Try to use loop-start signaling only for one-way trunks.

Trunk group related information

See the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207, for information on the types of circuit packs available and their capacities.

See your server's Installation manual for circuit-pack installation instructions.

CO, FX, or WATS trunk group administration

Basic administration for Central Office (CO), Foreign Exchange (FX), and WATS trunk groups is identical, so we've combined instructions for all 3 in the following procedure. In most cases, Avaya recommends leaving the default settings in fields that aren't specifically mentioned in the following instructions. Your Avaya representative or network service provider can give you more information. Your settings in the following fields must match your provider's settings:

- Direction
- Comm Type
- Trunk Type

⚠ **Caution:**

Use the list above as a starting point and talk to your service provider. Depending on your particular application, you might need to coordinate additional administration with your service provider.

Preparing to add a CO, FX, or WATS trunk group

Procedure

Before you administer any trunk group, verify you have one or more circuit packs of the correct type with enough open ports to handle the number of trunks you need to add.

To find out what circuit packs you need, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

Adding a CO, FX, or WATS trunk group example

About this task

As an example, we will set up a two-way CO trunk group that carries voice and voice-grade data only. Incoming calls terminate to an attendant during business hours and to a night service destination the rest of the time. We're adding trunk group 5 as an example.

Procedure

1. Enter **`add trunk-group next`**.
2. In the **Group Type** field, type `co`.

   This field specifies the kind of trunk group you're creating.
3. In the **Group Name** field, enter `Outside calls`.

   This name will be displayed, along with the group number, for outgoing calls if you set the **Outgoing Display** field to `y`. You can type any name up to 27 characters long in this field.
4. In the **COR** field, enter `85`.

This field controls which users can make and receive calls over this trunk group. Assign a class of restriction that's appropriate for the COR calling permissions administered on your system.

5. In the **TAC** field, enter`105`.

   This field defines a unique code that you or your users can dial to access this trunk group. The code also identifies this trunk group in call detail reports.

6. In the **Direction** field, enter `two-way`.

   This field defines the direction of traffic flow on this trunk group.

7. In the **Night Service** field, enter `1234`.

   This field assigns an extension to which calls are routed outside of business hours.

8. In the **Incoming Destination** field, enter`attd`.

   This field assigns an extension to which incoming calls are routed during business hours. By entering attd in this field, incoming calls go to the attendant and the system treats the calls as Listed Directory Number calls.

9. In the **Comm Type** field, enter `voice`.

   This field defines whether a trunk group can carry voice, data, or both. Analog trunks only carry voice and voice-grade data.

10. In the **Trunk Type** field, enter `ground-start`.

    This field tells the system what kind of signaling to use on this trunk group. To prevent glare, Avaya recommends ground start signaling for most two-way CO, FX, and WATS trunk groups.

11. Press **Next Page** until you find the **Outgoing Dial Type** field.

12. In the **Outgoing Dial Type** field, enter `tone`.

    This field tells Communication Manager how digits are to be transmitted for outgoing calls. Entering tone actually allows the trunk group to support both dual-tone multifrequency (DTMF) and rotary signals, so Avaya recommends that you always put tone in this field.

13. In the **Trunk Termination** field, enter `rc`.

    Use `rc` in this field when the distance to the central office or the server at the other end of the trunk is more than 3,000 feet. Check with your service provider if you're not sure of the distance to your central office.

14. Select `Enter` to save your changes.

    Now you are ready to add trunks to this trunk group. See Adding trunks to a trunk group example.

DID trunk group administration

In most cases, Avaya recommends leaving the default settings in fields that aren't specifically mentioned in the following instructions. Your Avaya representative or network service provider can give you more information. For Direct Inward Dialing (DID) trunk groups, settings in the following fields *must* match your provider's settings:

- Direction
- Comm Type
- Trunk Type
- Expected Digits (only if the digits your provider sends do not match your dial plan)

⚠ **Caution:**

Use the list above as a starting point and talk to your service provider. Depending on your particular application, you might need to coordinate additional administration with your service provider.

Preparing to add a DID trunk group

Procedure

Before you administer any trunk group, verify you have one or more circuit packs of the correct type with enough open ports to handle the number of trunks you need to add.

To find out what circuit packs you need, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

⊕ **Tip:**

In the **DID/Tie/ISDN Intercept Treatment** field on the Feature-Related System Parameters screen, enter `attd`. Incoming calls to invalid extensions will be routed to the attendant.

Adding a DID trunk group example

Procedure

1. Enter **`add trunk-group next`**.

The system assigns the next available trunk group number to this group. In our example, we're adding trunk group 5.

2. In the **Group Type** field, enter`did`.

   This field specifies the kind of trunk group you're creating.

3. In the **Group Name** field, enter `Incoming calls`.

   You can type any name up to 27 characters long in this field.

4. In the **COR** field, enter `85`.

   This field controls which users can receive calls over this trunk group. Assign a class of restriction that's appropriate for the COR calling permissions administered on your system.

5. In the **TAC** field, enter `105`.

   This code identifies the trunk group on CDR reports.

6. In the **Trunk Type** field, type wink-start.

   This field tells the system what kind of signaling to use on this trunk group. In most situations, use wink start for DID trunks to minimize the chance of losing any of the incoming digit string.

7. In the **Incoming Dial Type** field, enter `tone`.

   This field tells Communication Manager how digits are transmitted for incoming calls. Entering tone actually allows the trunk group to support both DTMF and rotary signals, so Avaya recommends that you always put tone in this field.

8. In the **Trunk Termination** field, enter`rc`.

   Use `rc` in this field when the distance to the central office or the server at the other end of the trunk is more than 3,000 feet. Check with your service provider if you're not sure of the distance to your central office.

9. Select `Enter` to save your changes.

   Now you're ready to add trunks to this trunk group. See Adding trunks to a trunk group example.

   See Digit insertion and absorption with trunk groups for instructions on matching modifying incoming digit strings to match your dial plan.

PCOL trunk group administration

In most cases, when administering Personal Central Office Line (PCOL) trunk groups, Avaya recommends leaving the default settings in fields that aren't specifically mentioned in the following instructions. Your Avaya representative or network service provider can give you more information. Your settings in the following fields must match your provider's settings:

- Trunk Type
- Trunk Direction

⚠ **Caution:**

Use the list above as a starting point and talk to your service provider. Depending on your particular application, you might need to coordinate additional administration with your service provider.

Preparing to add a PCOL trunk group

Procedure

Before you administer any trunk group, verify you have one or more circuit packs of the correct type with enough open ports to handle the number of trunks you need to add.

To find out what circuit packs you need, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

Adding a PCOL trunk group example

About this task

As an example, we will set up a new PCOL group and administer the group as a CO trunk for two-way voice traffic.

Procedure

1. Enter **`add personal-co-line next`**.
2. In the `Group Type` field, enter `co`.

   This field specifies the kind of trunk group you're creating. PCOL groups can be administered as CO, FX, or WATS trunks.
3. In the **Group Name** field, enter `Outside calls`.

   This name will be displayed, along with the group number, for outgoing calls if you set the **Outgoing Display** field to `y`. You can type any name up to 27 characters long in this field. (You might want to put the telephone number here that's assigned to this trunk.)
4. In the **TAC** field, enter **111**.

This field defines a unique code that you or your users can dial to access this trunk group. The code also identifies this trunk group in call detail reports.

5. In the **Trunk Type** field, enter `ground start`.

   This field tells the system what kind of signaling to use on this trunk group. To prevent glare, Avaya recommends ground start signaling for most two-way CO, FX, and WATS trunk groups.

6. In the **Trunk Port** field, enter `01D1901`.

   This is the port to which the trunk is connected.

7. In the **Trunk Termination** field, enter `rc`.

   Use `rc` in this field when the distance to the central office or the server at the other end of the trunk is more than 3,000 feet. Check with your service provider if you're not sure of the distance to your central office.

8. In the **Outgoing Dial Type** field, enter `tone`.

   This field tells Communication Manager how digits are to be transmitted for outgoing calls. Entering tone actually allows the trunk group to support both DTMF and rotary signals, so Avaya recommends that you always put tone in this field.

9. Select `Enter` to save your changes.

   You assign telephones to a PCOL group by administering a CO Line button on each telephone. Once assigned, the Assigned Members page of the Personal CO Line Group screen displays member telephones:

PCOL trunk group interactions

Call Detail Recording PCOL interaction

Call detail recording (CDR) can be activated for calls on a personal CO line, but the CDR record does not specifically identify the call as PCOL. Calls over personal CO lines can, however, be identified by the trunk access code used on the call. The call is recorded to the extension number assigned to the telephone where the call was originated or answered.

PCOL restrictions

- Abbreviated Dialing can be used with a personal CO line, but the accessed lists are associated with the individual telephones.
- Auto Hold and Leave Word Calling do not work with calls on a personal CO line.
- Send All Calls cannot be activated for a personal CO line.

- Communication Manager Messaging cannot be in the coverage path of a PCOL group.
- Only telephones in the same PCOL group can bridge onto calls on the personal CO line. If a user is active on his or her primary extension number on a PCOL call, bridged call appearances of that extension number cannot be used to bridge onto the call.
- When a user puts a call on hold on a personal CO line, the status lamp associated with the PCOL button does not track the busy/idle status of the line.

Tie or Access trunk group administration

In most cases, Avaya recommends leaving the default settings in fields that aren't specifically mentioned in the following instructions. Your Avaya representative or network service provider can give you more information. Your settings in the following fields must match your provider's settings (or the setting on the far-end server, if this is a private network trunk group):

- Direction
- Comm Type
- Trunk Type

⚠ **Caution:**

Use the list above as a starting point and talk to your service provider. Depending on your particular application, you might need to coordinate additional administration with your service provider.

Preparing to add a Tie or Access trunk group

Procedure

Before you administer any trunk group, verify you have one or more circuit packs of the correct type with enough open ports to handle the number of trunks you need to add.

To find out what circuit packs you need, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

⊕ **Tip:**

In the **DID/Tie/ISDN Intercept Treatment** field on the Feature-Related System Parameters screen, enter `attd`. Incoming calls to invalid extensions get routed to the attendant.

Adding a Tie or Access trunk group example

About this task

As an example, we will add a two-way tie trunk group that supports voice and voice-grade data. We're adding trunk group 5.

Procedure

1. Enter `add trunk-group next`.
2. In the **Group Type** field, enter `tie`.

   This field specifies the kind of trunk group you're creating.
3. In the **Groncup Name** field, enter `Outside calls`.

   This name will be displayed, along with the group number, for outgoing calls if you set the **Outgoing Display** field to `y`. You can type any name up to 27 characters long in this field.
4. In the **COR** field, enter `85`.

   This field controls which users can make or receive calls over this trunk group. Assign a class of restriction that's appropriate for the COR calling permissions administered on your system.
5. In the **TAC** field, enter `105`.

   This field defines a unique code users can dial to access this trunk group.
6. In the **Direction** field, enter `two-way`.

   This field defines the direction of traffic flow on this trunk group.
7. In the **Night Service** field, enter `1234`.

   This field assigns an extension to which calls are routed outside of business hours.
8. In the **Comm Type** field, enter `voice`.

   This field defines whether a trunk group can carry voice, data, or both. Analog trunks only carry voice and voice-grade data. If you're administering a T1 connection in North America, enter `rbavd` in this field.
9. In the **Trunk Type** field, enter `wink/wink`.

   This field tells the system what kind of signaling to use on this trunk group. Because we're receiving and sending digits over this trunk group, we're using wink/wink signaling to minimize the chance of losing part of the digit string in either direction.
10. Enter `tone` in both the **Outgoing Dial Type** and **Incoming Dial Type** fields.

These fields tell Communication Manager how digits are transmitted for incoming calls. Entering tone actually allows the trunk group to support both DTMF and rotary signals, so Avaya recommends that you always put tone in this field.

11. Select `Enter` to save your changes.

    Now you're ready to add trunks to this trunk group. See Adding trunks to a trunk group example.

DIOD trunk group administration

Administration for Direct Inward and Outward Dialing (DIOD) trunk groups varies from country to country. See your local Avaya representative for more information. Remember that the central office serving your switching system might be emulating another country's network protocol. If so, you'll have to administer your circuit packs and trunk groups to match the protocol used by your central office.

If you are using Incoming Caller ID (ICLID) on analog trunks connected to a DIOD Central Office trunk circuit pack, DO NOT put these trunks in an outgoing AAR or ARS route pattern. Since the loop-start trunks supported on the DIOD Central Office trunk circuit pack do not provide answer supervision, the potential for toll fraud exists.

Digital trunks administration

Any of the common trunks, except for PCOL trunks, can be analog or digital. (PCOL trunks can only be analog.) Administering a digital trunk group is very similar to administering its analog counterpart, but digital trunks must connect to a DS1 circuit pack and this circuit pack must be administered separately. The example in this section shows you how to do this.

In most cases, Avaya recommends leaving the default settings in fields that aren't specifically mentioned in the following instructions. Your Avaya representative or network service provider can give you more information.

Your settings in the following fields must match your provider's settings:

- Bit Rate
- Line Coding (unless you're using a channel service unit to convert between your line coding method and your provider's)
- Framing Mode
- Signaling Mode
- Interface Companding

⚠ **Caution:**

> Use the list above as a starting point and talk to your service provider. Depending on your particular application, you might need to coordinate additional administration with your service provider.

See DS1 Circuit Pack in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for information on administering DS1 service.

See DS1 Trunk Service in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information on DS1 service.

Preparing to add a digital trunk

Procedure

1. Assign the DS1 circuit pack before you administer the members of the associated trunk groups.

   ⚠ **Caution:**

   > If enhanced DS1 administration is not enabled, you cannot make changes to the DS1 Circuit Pack screen before you remove related member translations of all trunks from the trunk group. See Enhanced DS1 administration.

2. Before you administer a digital trunk group, verify you have one or more circuit packs that support DS1 with enough open ports to handle the number of trunks you need to add.

   To find out what circuit packs you need, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

Configuring a DS1 circuit pack example

About this task

The following example shows a DS1 circuit pack configured for T1 service. The circuit pack is supporting a two-way CO trunk group that carries only voice and voice-grade data.

To configure a new DS1 circuit pack:

Procedure

1. Enter **`add ds1 07A19`**.

   You must enter a specific port address for the circuit pack.

2. In the **Name** field, enter `two-way CO`.

   Use this name to record useful information such as the type of trunk group associated with this circuit pack or its destination.

3. In the **Bit Rate** field, enter `1.544`

   (Standard for T1 lines).

4. In the **Line Coding** field, enter `b8zs`.

   Avaya recommends you use `b8zs` whenever your service provider supports it. Since this trunk group only carries voice traffic, you could also use `ami-zcs` without a problem.

5. In the **Framing Mode** field, enter `esf`.

   Avaya recommends you use `esf` whenever your service provider supports it.

6. In the **Signaling Mode** field, enter `robbed-bit`.

7. In the **Interface Companding** field, enter `mulaw`.

   This is the standard for T1 lines in North America.

8. Select **Enter** to save your changes.

Recommended T1 and E1 settings

T1 recommended settings

The table below shows recommended settings for standard T1 connections to your local exchange carrier.

Field	Value	Notes
Line Coding	`b8zs`	Use `ami-zcs` if `b8zs` is not available.
Signaling Mode	`robbed-bit`	Robbed-bit signaling gives you 56K bandwidth per channel. If you need a 64K clear channel for applications like asynchronous data transmission or remote administration access, use common channel signaling.
Framing	`esf`	Use `d4` if `esf` is not available.

If you use b8zs line coding and esf framing, it will be easier to upgrade your T1 facility to ISDN should you want to. You can upgrade without reconfiguring external channel service units, and your service provider won't have to reconfigure your network connection.

E1 recommended settings

DS1 administration for E1 service varies from country to country. See your local Avaya technical support representative for more information.

Note:

Remember that the central office serving your switching system might be emulating another country's network protocol. If so, you'll have to administer your circuit packs and trunk groups to match the protocol used by your central office.

Enhanced DS1 administration

Normally, you can't change the DS1 Circuit Pack screen unless you remove all related trunks from their trunk group. However, if the **DS1 MSP** field on the System-Parameters Customer-Options (Optional Features)screen is `y`, and you are assigned the associated login permissions, you can change some of the fields on the DS1 Circuit Pack screen without removing the related trunks from their trunk group.

If you busy out the DS1 circuit pack, you can change the following fields: **CRC**, **Connect**, **Country Protocol**, **Framing Mode**, **Interface**, **Interconnect**, **Line Coding**, and **Protocol Version**.

After changing these fields, you might also have to change and resubmit associated screens.

Enhanced DS1 administration matched field settings

For enhanced DS1 administration, some field values on the DS1 Circuit Pack screen must be consistent with those on other screens as shown in the table below. If you change field values on the DS1 Circuit Pack screen, you must change the related fields on the other screens and resubmit them.

DS1 Circuit Pack field	Affected screens[1]
Line Coding	Route Pattern Access Endpoint Signaling Group Tone Generation
Connect	Signaling Group
Protocol Version	Signaling Group

[1] See *Avaya Aura™ Communication Manager Screen Reference*, 03-602878

DS1 Circuit Pack field	Affected screens[1]
Interface	Signaling Group
Interconnect	Tone Generation
Country Protocol	Signaling Group Tone Generation

Specific combinations of settings for some of these fields are shown below.

ITC, Bit Rate, and Line Coding values for enhanced DS1 administration

The **ITC (Information Transfer Capability)** field appears on the Route Pattern screen, Trunk Group screen, and Access Endpoint screen. The **Line Coding** and the **Bit Rate** fields appear on the DS1 Circuit Pack screen. The settings for these fields on all the screens must be coordinated as shown in the following tables.

ITC field	Bit Rate	Line Coding field
restricted	1.544 Mbps	ami-zcs
	2.048 Mbps	ami-basic
unrestricted	1.544 Mbps	b8zs
	2.048 Mbps	hdb3

Interconnect and Group Type entries for enhanced DS1 administration

The **Interconnect** field appears on the DS1 Circuit Pack screen. The **Group Type** field appears on the Trunk Group screen. Set these fields as shown in the following table.

Interconnect field	Group Type field
co	co, did, diod, fx, or wats
pbx	access, aplt, isdn-pri, tandem, or tie

[1] See *Avaya Aura™ Communication Manager Screen Reference*, 03-602878

Adding trunks to a trunk group example

About this task

Use this procedure to add new trunks or to change the assignment of existing trunks. To change the assignment of existing trunks, remove them from their current trunk group and add them to the new group.

You must add a trunk group before you can assign and administer individual trunks. To add a new trunk group, see the instructions in this chapter for the type of group you want to add.

As an example, we will assign 5 trunks to a new tie trunk group, trunk group 5. We'll use ports on several circuit packs for members of this group.

Procedure

1. Enter `change trunk-group 5`.
2. Click **Next Page** to move to the Group Member Assignments screen.

   Some of the fields on this screen do not appear for every trunk group.
3. In the **Port** field in row 1, enter `1B1501`.

   This field assigns the first member of the trunk group to a port on a circuit pack.
4. In the **Name** field in row 1, enter `5211`.

   This is the extension assigned to this trunk. In general, type the circuit ID or telephone number for each trunk in this field. The information is helpful for tracking your system or troubleshooting problems. Update these fields whenever the information changes.
5. In the **Mode** field, enter `e&m`.

   ⚠ **Caution:**

   An entry in this field is only required for some circuit packs. Dip switch settings on the circuit pack control the signalling mode used on the trunk group, so the entry in the Mode field must correspond to the actual setting on the circuit pack.
6. In the **Type** field, enter `t1-comp`.

   An entry in this field is only required for some circuit packs.
7. Repeat steps 3 to 6, as appropriate, for the remaining trunks.

   Notice that you can assign trunks in the same trunk group to ports on different circuit packs.
8. Select `Enter` to save your changes.

Removing trunk groups example

About this task

There's more to removing a trunk group than just executing the **`remove trunk-group`** command. If you're using Automatic Route Selection (ARS), you must remove an outgoing or two-way trunk group from any route patterns that use it. If you've administered **Trunk-Group Night Service** buttons for the trunk group on any telephones, those buttons must be removed or assigned to another trunk group.

As an example, we will remove trunk group 5. This two-way group is used in ARS route pattern 2. In addition, a **Trunk-Group Night Service** button on extension 8410 points to this group.

Procedure

1. In the Route Pattern screen for route pattern 2, clear the entries for trunk group 5.

   If you're replacing trunk group 5 with another trunk group, just type the information for the new trunk group over the old entries. Remember to press `Enter` to save your changes.
2. In the Station screen for extension 8410, clear the entry in the **BUTTON ASSIGNMENTS** field for the **Trunk-Group Night Service** button.
3. Select `Enter` to save your changes.
4. In the `Group Member Assignments` screen for trunk group 5, remove all member trunks from the group.

   See Adding trunks to a trunk group example for instructions.
5. Enter **`remove trunk-group 5`**.
6. Select `Enter` to remove the trunk group.

Trunk resets

To "reset" a trunk, use the **`busyout`** command followed by the **`release`** command, both executed in a SAT window. You can run these commands on a board, a port, a trunk group, or an individual trunk. The availability of these commands depends on your login permissions.

Note:

These commands can tear calls down, so use them with great caution. Contact your Avaya technical representative for details.

Resetting a trunk group

Procedure

1. Enter `busyout trunk` **`n`**, where **`n`** is the number of the trunk group.
2. Enter **`release trunk`** `n`.

   The trunk group is reset. (Example: **`busyout trunk 43`** followed by **`release trunk 43`**.)

Resetting a trunk member

Procedure

1. Enter `busyout trunk` *`n/x`*, where *n* is the number of the trunk, and *x* is the trunk group member.
2. Enter `release trunk` **`n/x`**.

   The trunk group member is reset. (Example: **`busyout trunk 43/1`** followed by **`release trunk 43/1`**. Another example operation for an ISDN trunk is **`test trunk 43`**.)

Digit insertion and absorption with trunk groups

Use these procedures to modify the incoming digit string on DID and tie trunks by inserting (adding) or absorbing (deleting) digits. You'll need to do this if the number of digits you receive doesn't match your dial plan.

See DID trunk group administration for instructions on administering a DID trunk group.

See Tie or Access trunk group administration for instructions on administering a tie trunk group.

Inserting digits with trunk groups example

About this task

As an example, let us say you have a DID trunk group. It's group number is 5. Your service provider can only send 4 digits, but your dial plan defines 5-digit extensions beginning with 6:

Procedure

1. Enter `change trunk-group 5`.
2. In the **Digit Treatment** field, enter `insertion`.

   This field tells Communication Manager to add digits to the incoming digit string. These digits are always added at the beginning of the string.
3. In the **Digits** field, enter`6`.

   For insertion, this field defines the specific digits to insert. Communication Manager will add a “6” to the front of the digit strings delivered with incoming calls. For example, if the central office delivers the string “4444,” Communication Manager will change it to “64444,” an extension that fits your dial plan.
4. In the Expected Digits field, enter `4`.

   This field tells Communication Manager how many digits the central office sends.

   Note:

   The **Expected Digits** field does not appear on the screen for tie trunk groups.
5. Select `Enter` to save your changes.

Absorbing digits with trunk groups example

About this task

If your service provider sends 7 digits but you only need 5, you need to absorb the first 2 digits in the digit string.

Procedure

1. Enter `change trunk-group 5`.
2. In the **Digit Treatment** field, enter `absorption`.

   This field tells Communication Manager to remove digits from the incoming digit string. These digits are always removed from the beginning of the string.
3. In the **Digits** field, enter `2`.

   For absorption, this field defines how many digits will be absorbed. Communication Manager will remove the first 2 digits from the digit strings delivered with incoming calls. For example, if the central office delivers the string “556-4444,” Communication Manager will change it to “64444,” an extension that fits your dial plan.

4. In the **Expected Digits** field, enter `7`.

   This field tells Communication Manager how many digits the central office sends.

   Note:

   The **Expected Digits** field does not appear on the screen for tie trunk groups.

5. Select `Enter` to save your changes.

Administering trunks for LDN example

About this task

Listed directory numbers (LDN) are the telephone numbers given for an organization in public telephone directories. You can administer Communication Manager so that calls to different listed directory numbers go to the same attendant group. How you administer your system for LDN calls depends on whether the calls are coming in over DID and tie trunks or over CO and FX trunks.

As an example, let us say that one attendant group answers calls for 3 different businesses, each with its own listed directory number:

Procedure

1. Company A — 855-2020
2. Company B — 855-1000
3. Company C — 855-1111

   DID trunks and some tie trunks transmit part or all of the dialed digit string to Communication Manager. If you want these calls to different numbers to go to one attendant group, you must identify those numbers for Communication Manager on the Listed Directory Numbers screen.

   We will take the 3 businesses listed above as an example. We will assume your server receives 4 digits from the central office on a DID trunk group and that you’re not using Tenant Partitioning. To make these calls to different listed directory numbers terminate to your attendant group:

   a. Enter `change listed-directory-numbers`.

   b. In the **Ext 1** field, enter`2020`.

      This is the LDN for Company A.

c. In the **Name** field, enter `Company A`.

   This name appears on the console display so the attendant knows which business the call is for and how to answer it.

d. Repeat steps 2 and 3 for the other two businesses.

   You can enter up to 20 different listed directory numbers on this screen.

e. Select `Enter` to save your changes.

To make LDN calls over a CO or FX trunk group terminate to an attendant group, you must type attd in the **Incoming Destination** field on the Trunk Group creen for that group.

When you use the Listed Directory Number screen to assign some extensions to the attendant group, or when you enter `attd` in the **Incoming Destination** field on the Trunk Group screen for CO or FX trunks, Communication Manager treats these calls as LDN calls.

See Listed Directory Numbers in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for detailed information about this feature.

Answer Detection Administration

Use this procedure to administer an outgoing or two-way trunk group for network answer supervision or answer supervision by timeout. If your network supplies answer supervision to a trunk group, you can administer Communication Manager to recognize and respond to that signal. If your network does not supply answer supervision, you can set a timer for all calls on that group. When the timer expires, Communication Manager assumes the call has been answered and call detail recording starts (if you are using CDR).

For information about answer detection by call classification, contact your Avaya technical support representative or see Answer Detection in *Avaya Aura™™ Communication Manager Feature Description and Implementation*, 555-245-205 for an introduction.

Preparing to administer Answer Detection

Procedure

Determine whether the trunk group receives answer supervision from your service provider or private network.

For example, most loop-start CO, FX, and WATS trunks do not provide answer supervision.

Administering Answer Detection example

About this task

As an example, we will administer trunk group 5 for both types of answer detection.

Procedure

1. On the Trunk Group screen for group 5, enter `y` in the **Receive Answer Supervision** field.
2. Select `Enter` to save your change.

   Now we will administer answer supervision by timeout. We'll set the timer to 15 seconds.

   a. On the Trunk Group screen for group 5, type `15` in the **Answer Supervision Timeout** field.

   b. Select `Enter` to save your change.

   See Answer Detection in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information about this feature.

ISDN trunk groups Administration

Integrated Services Digital Network (ISDN) trunk groups support the ISDN and Call-by-Call Service Selection service selection features. The trunk group provides end-to-end digital connectivity and supports a wide range of services including voice and non-voice services, to which users have access by a limited set of CCITT-defined, standard multipurpose interfaces.

The ISDN trunk group can contain ISDN-PRI or ISDN-BRI interfaces. However, it is not possible to use the two types of interfaces in the same trunk groups. The type of interface is chosen when the trunk members are assigned to the trunk group.

When ISDN-PRI interfaces are used on ISDN trunk groups, they can also be used to support the Wideband Switching feature. This is intended to work with the H0 (384 Kbps), H11 (1536 Kbps), H12 (1920 Kbps), and NXDS0 (128 to 1984 Kbps) data services, and to support high-speed video conferencing and data applications.

When an ISDN trunk connects two servers or switches, set the trunk options identically at both ends of the connection, with the exception of the **Trunk Hunt** fields. When ISDN-PRI interfaces are used, it is acceptable for both ends to have the **Trunk Hunt** fields administered as cyclical, but if one end is administered as ascend, the other end must be administered as descend. This helps avoid the possibility of glare conditions. When ISDN-BRI is used, the **Trunk Hunt** field has to be cyclical.

ISDN trunk group hardware requirements

ISDN-BRI trunk interfaces are supported by all of these:

- The TN2185 Trunk-side BRI circuit pack and the MM722 BRI circuit pack implement the user side of the BRI trunk interface.
- The TN556B/C/D ISDN-BRI Line circuit pack and the TN2198 ISDN BRI (U-LT) Line circuit pack implement the network side of the BRI trunk interface.
- The MM720 BRI circuit pack implements both sides of the interface. You can select the options from the BRI Trunk Circuit Pack screen

For BRI trunk connections to a public ISDN, use the TN2185, MM722, or MM720. For BRI tie trunks between systems, use the TN2185, MM722, or MM720 on one side and the TN556B/C/D or TN2198 on the other side. The TN2464 circuit supports T1 and E1 digital facilities.

ISDN-PRI interfaces are supported by the TN767 circuit pack (for assignment of a T1 signaling link and up to 24 ISDN-PRI trunk group members), or the TN464C or later circuit pack (for assignment of a T1 or E1 signaling link and up to 24 or 31 ISDN-PRI trunk group members, respectively). The TN2464 and TN2207 circuit pack can also be used with ISDN-PRI.

- The D-channel for ISDN-PRI interfaces switches through either the TN765 Processor Interface (PI) circuit pack or the TN778 Packet Control (PACCON) circuit pack. The D-channel for ISDN-BRI interfaces only switches through the TN778 Packet Control (PACCON) circuit pack.

  Note:

  You cannot use the TN765 circuit pack with ISDN-BRI interfaces.
- A TN780 or TN2182 Tone Clock circuit pack provides synchronization for the DS1 circuit pack.

Note:

The TN767 cannot be used to carry the D-channel if either the TN778 (PACCON) or TN1655 (PKTINT) circuit packs are used to switch the D-channel. However, in these circumstances, the TN767 can be used for NFAS interfaces carrying only B-channels.

Screens used to administer ISDN trunk groups

Screen	Field
Feature-Related System Parameters	**Send Non-ISDN Trunk Group Name as Connected Name?** **Display Connected Name/Number for ISDN DCS Calls?**
Incoming Call Handling Treatment	All
Numbering - Public/Unknown Format	**All**
System Parameters Customer-Options (Optional Features)	**Version** **ISDN-BRI Trunks** **ISDN-PRI** **QSIG Optional Features**
Synchronization Plan	**All**
Trunk Group (ISDN)	**All**
ISDN-BRI Circuit Pack screen (if using ISDN-BRI interfaces) or DS1 Circuit Pack screen (if using ISDN-PRI interfaces)	**All** **All**
ISDN Numbering - Private	**All**
Route Pattern	**All**
Hunt Groups	**ISDN Caller Display**
Signaling Group (if using ISDN-PRI interfaces)	**All**
Terminating Extension Group	**ISDN Caller Display**

Table Notes:

- System Parameters Customer-Options (Optional Features) — The **ISDN-BRI Trunks** or **ISDN-PRI** fields must be set to y. For a TN778 and if using ISDN-PRI interfaces, the **PRI Over PACCON** field must be set to y. These features are provided via license file. To enable these features, contact your Avaya representative.
- **QSIG Optional Features** fields can be enabled to allow appropriate administration for Supplementary Service Protocol.
- Feature-Related System-Parameters — Set the **Send Non-ISDN Trunk Group Name** as **Connected Name** and **Display Connected Name/Number for ISDN DCS Calls** fields.
- ISDN-BRI Trunk Circuit Pack — This screen is required if using ISDN-BRI trunk interfaces. Assign all fields as required.

- DS1 Circuit Pack — This screen is required if using ISDN-PRI interfaces.
    - DS1 (T1) Circuit Pack

      Assign all fields as required. For **Facility Associated Signaling**, up to 23 ports are available for administration as trunk members in an associated ISDN-PRI trunk group. The 24th port is used as a signaling channel. For **Non-Facility Associated Signaling**, all 24 ports can be used on certain DS1 circuit packs. The D-channel signaling function for these packs must be provided by a designated DS1 pack on its 24th channel.
    - E1 Circuit Pack

      Assign all fields as required. For **Facility Associated Signaling**, up to 30 ports are available for administration as trunk members in an associated ISDN-PRI trunk group. Port number 16 is used as a signaling channel.
- Maintenance-Related System-Parameters — Use this screen only for a TN778. Set the **Packet Bus Maint** field to `y`.
- ISDN Trunk Group — Enter information in all the fields except the trunk group members. When using ISDN-PRI interfaces, enter the members after you establish the signaling links.
- Signaling Group — This screen is required if ISDN-PRI interfaces are used. Complete all fields. This screen identifies groups of ISDN-PRI DS1 interface B-channels for which a given D-channel (or D-channel pair) will carry the associated signaling information (supports the Facility and Non-Facility Associated Signaling feature). Each DS1 board that is required to have a D-channel must be in a different signaling group by itself (unless D-channel backup is needed, in which case a second DS1 is administered as a backup D-channel). You are not required to select a channel for a trunk group, but if you do, you must have already defined the trunk group as type ISDN.

Note:

The following three screens, Processor Interface Data Module, Communication Interface Links, and Communication Processor Channel Assignment are used only to support the ISDN-PRI interfaces using PI TN765.

- Processor Interface Data Module — Use this screen only for a TN765. Assign up to 8 interface links using 8 Processor Interface Data Module screens for multi-carrier cabinet systems, and up to 4 links for single-carrier cabinet systems. One Processor Interface Data Module screen must be completed for each interface link to be assigned.
- Communication Interface Links — Use this screen only for a TN765. Assign link numbers 01 to 08 for a multi-carrier cabinet system or links 01 to 04 for a single-carrier cabinet system as required. When first administering this screen for ISDN in Communication Manager, do not administer the **Enable** field.
- Communication Processor Channel Assignment — Use this screen only for a TN765. Enter assigned link numbers and assign associated channel numbers to each link. Complete all fields of the screen as required. When first administering this screen for ISDN in Communication Manager, you need to:
    - First, administer the Interface Links screen, except the **Enable** field.

  - Second, administer the **ISDN** fields on the **Processor Channel** screen.
  - Last, go back to the Interface Links screen and administer the **Enable** field.
- ISDN Numbering - Public/Unknown — Complete all fields. This screen supports the ISDN Call Identification Display.
- ISDN Numbering - Private — Complete all fields. This screen supports the ISDN Call Identification Display.
- Routing Pattern — Complete all fields including the **Supplemental ISDN Routing Information** fields as required.
- Hunt Group — Complete the **ISDN Caller Display** field by entering either `grp-name` or `mbr-name` to specify whether the hunt group name or member name, respectively, is sent to the originating user (supports the ISDN Call Identification Display feature).
- Terminating Extension Group — Complete the **ISDN Caller Display** field by entering either `grp-name` or `mbr-name` to specify whether the group name or member name, respectively, is sent to the originating user (supports the ISDN Call Identification Display feature).
- Synchronization Plan — Assigns primary and secondary external synchronization sources for the ISDN-BRI Trunk or DS1 circuit pack. Complete all screen fields as required.

Note:

ISDN-BRI and ISDN-PRI interfaces cannot be mixed in the same trunk group. Therefore, consider the following:

- The earliest trunk member (the lowest numbered one) administered is considered correct.
- If an offending member is subsequently found (meaning the first member was BRI and a later member was PRI, or vice versa), the cursor positions on the offending member, and the following error message appears: `You cannot mix BRI and PRI ports in the same trunk group.`

Administering displays for QSIG trunks

Procedure

1. On the Trunk Group screen set the following fields:
   - **Group Type**: ISDN
   - **Character Set for QSIG Names**: iso8859-1
   - **Outgoing Display**: y
   - **Send Calling Number**: y
2. On the Signaling Group screen set the following fields:
   - **Supplementary Service Protocol**: b

3. On the System-Parameters Country-Options screen set the following field:
   - **Display Character Set**: Roman

QSIG over SIP

Use the QSIG over SIP (Q-SIP) feature to enable calls between two Communication Manager systems interconnected by an IP network that uses SIP signaling with the full range of QSIG functionality.

Preparing to administer QSIG over SIP

Before you begin

Ensure that the system is running Communication Manager Release 6.0 or later. Release 6.0 or later is required on all nodes that participate in Q-SIP calls. The nodes can be originating, tandem, or terminating.

Procedure

1. Enter `display system-parameters customer-options`.
2. Click **Next** until you find the **Maximum Administered IP Trunks** field.
3. Ensure that the **Maximum Administered IP Trunks** field is set to greater than 1 and include enough trunks for Q-SIP trunk group use.
4. Click **Next** until you find the **Maximum Administered SIP Trunks** field.
5. Ensure that the **Maximum Administered SIP Trunks** field is set to greater than 1 and include enough trunks for Q-SIP trunk group use.
6. Scroll through the screens to find the **IP Trunks** field.
7. Ensure that the **IP Trunks** field is set to `y`.

   Note:

   If the **Maximum Administered IP Trunks** and **Maximum Administered SIP Trunks** fields are set to less than 1, or the **IP Trunks** field is set to n, your system is not enabled for the QSIG over SIP feature. Contact your Avaya representative for assistance.
8. Select **Enter** to exit the screen.

Administration of the QSIG and SIP trunk and signaling groups

You must administer the following trunks on each node:

- H.323 IP trunk equipped with QSIG signaling
- SIP trunk equipped with SIP signaling

You must administer the required number of QSIG and SIP trunk group members.

For information on creating the QSIG and SIP trunk and signaling groups, see the Administering IP trunks section of *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

Note:

When creating the QSIG and SIP trunk groups, do not add trunk members to these trunk groups. Add the trunk members to the trunk groups after changing the QSIG and SIP trunk groups.

Note:

You must configure the Far-end Node Name of the QSIG signaling group, though the QSIG trunk serves as the feature layer and has no Far End. Due to the missing Far end, a dummy ip-node name must be used with the same IP address, which is already used for the Near End. You need to define this dummy ip-node name in the IP node name table before creating the QSIG signaling group.

Note:

If you create a new QSIG signaling group, must not use the default port 5060.

For Q-SIP you must specifically change the QSIG and SIP trunk and signaling groups. This is described in the following sections.

Changing the QSIG and SIP signaling groups for Q-SIP

Before you begin

Ensure that the QSIG and SIP signaling groups exist.

About this task

- Change the QSIG signaling group.
- Change the SIP signaling group.

Changing the QSIG signaling group

Procedure

1. Enter `change signaling-group n`, where *n* is the signaling group number, for example, *n* = 18.
2. Set the **Q-SIP** field to `y`.

   By default, the Q-SIP feature is disabled. This field appears only when the **Group Type** field is set to SIP or H.323.
3. In the **SIP Signaling Group** field, type a valid entry.

   The valid entry must refer to an administered SIP signaling group. For example, if you have created SIP signaling group 17, the **SIP Signaling Group** field must refer to SIP signaling group 17. This field appears only when the **Q-SIP** field is set to y.
4. Select **Enter** to save your changes.

Changing the SIP signaling group

Procedure

1. Enter `change signaling-group n`, where *n* is the signaling group number, for example, *n* = 17.
2. Set the **Q-SIP** field to `y`.

   By default, the Q-SIP feature is disabled. This field appears only when the **Group Type** field is set to SIP or H.323.
3. In the **QSIG Signaling Group** field, type a valid entry.

   The valid entry must refer to an administered H.323 signaling group. For example, if you have created QSIG signaling group 18, the **QSIG Signaling Group** field must refer to QSIG signaling group 18. This field appears only when the **Q-SIP** field is set to y.
4. Select **Enter** to save your changes.

Changing the QSIG and SIP trunk groups for Q-SIP

Before you begin

Ensure that the QSIG and SIP trunk groups exist.

About this task

- Change the QSIG trunk group.
- Change the SIP trunk group.
- Add trunk group members to the QSIG trunk group.
- Add trunk group members to the SIP trunk group.

Changing the QSIG trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number, for example, *n* = 18.
2. Ensure that the **Group Type** field is `isdn` and **Carrier Medium** field is `H.323`.
3. Click **Next** until you see the QSIG Trunk Group Options section.
4. In the **SIP Reference Trunk Group** field, type a valid entry.

   The valid entry must refer to an administered SIP trunk group. For example, if you have created SIP trunk group 17, the **SIP Reference Trunk Group** field must refer to SIP trunk group 17.
5. Set the **TSC Method for Auto Callback** field to `drop-if-possible`.
6. Select **Enter** to save your changes.

Changing the SIP trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number, for example, *n* = 17.
2. Ensure that the **Group Type** field is set to `SIP`.
3. Click **Next** until you see the **Protocol Variations** section.
4. Set the **Enable Q-SIP** field to `y`.

   By default, the Q-SIP feature is disabled.
5. In the **QSIG Reference Trunk Group** field, type a valid entry.

   The valid entry must refer to an administered QSIG trunk group. For example, if you have created QSIG trunk group 18, the **QSIG Reference Trunk Group** field must refer to QSIG trunk group 18.

6. Select **Enter** to save your changes.

Adding trunk group members to the QSIG trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number, for example, *n* = 18.
2. Click **Next** until you see the Group Member Assignments section.
3. Add trunk group members to the numbered **Group Member Assignments**.
4. Select **Enter** to save your changes.

   ✱ **Note:**

   Instead of adding the trunk group members on the **Group Member Assignments**, you can set the **Member Assignment Method** field to `auto` and set the Number of Members.

Adding trunk group members to the SIP trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number, for example, *n* = 17.
2. Click **Next** until you see the Group Member Assignments section.
3. Add trunk group members to the numbered **Group Member Assignments**.
4. Select **Enter** to save your changes.

   ✱ **Note:**

   Instead of adding the trunk group members on the **Group Member Assignments**, you can set the Number of Members.

Routing of QSIG over SIP

Procedure

From the caller or calling party point of view, only the QSIG trunk is seen and used for routing, for example, in the route pattern. The SIP trunk is not seen and must not be used for routing.

Verifying a Q-SIP test connection

Procedure

1. Establish a Q-SIP call.
2. Type `status trunk QSIG-group-number`, where *QSIG-group-number* is the QSIG trunk group number in use.

   You must remember the active trunk group member for verifying a Q-SIP connection.
3. Type `status trunk QSIG-group-number/member-number`, where *QSIG-group-number* is the QSIG trunk group number and *member-number* is the QSIG trunk group member number, which you have identified in step 2. Press `Enter`.
4. On the Trunk Status screen, if a station is connected to a QSIG over SIP trunk, you can view the involved port of the QSIG trunk in the **Q-SIP Reference Port** field.
5. Type `status station n`, where *n* is the extension of the station.
6. On the General Status screen, if a station is connected to a QSIG over SIP trunk, you can view the involved port of the SIP trunk in the **Connected Ports** field. However, you cannot view the port of the QSIG trunk because the port is not involved in the media connection.

   See the description of the Connected Ports field in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431, for more information.
7. Press `Enter` to exit the screen.

Removing the Q-SIP configuration

Disabling Q-SIP for the QSIG signaling group

Procedure

1. Enter `change signaling-group n`, where *n* is the signaling group number, for example, *n* = 18.
2. Set the **Q-SIP** field to `n`.
3. Select **Enter** to save your changes.

Disabling Q-SIP for the SIP signaling group

Procedure

1. Enter `change signaling-group n`, where *n* is the signaling group number, for example, *n* = 17.
2. Set the **Q-SIP** field to `n`.
3. Select **Enter** to save your changes.

Disabling Q-SIP for the QSIG trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number, for example, *n* = 18.
2. Click **Next** until you see the QSIG Trunk Group Options section.
3. Set the **SIP Reference Trunk Group** field to `blank`.
4. Select **Enter** to save your changes.

Disabling Q-SIP for the SIP trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the number of the trunk group number, for example, *n* = 17.
2. Click **Next** until you see the Protocol Variations section.
3. Set the **Enable Q-SIP** field to *n*.
4. Select **Enter** to save your changes.

Chapter 16: Managing Announcements

An announcement is a recorded message a caller can hear while the call is in a queue, or if a call receives intercept treatment for some reason. An announcement is often used in conjunction with music.

The source for announcements can be either integrated or external.

- Integrated announcements reside on a circuit pack in the carrier, such as the TN2501AP circuit pack, or embedded in a media gateway processor board (called a “v VAL source” throughout this chapter).
- External announcements are stored on a separate piece of equipment (called an “adjunct”), and played back from the adjunct equipment.

This chapter uses the term “announcement source” to mean either integrated or external sources for announcements.

VAL or Media Gateway Virtual VAL resources

Before you can use the capabilities of the VAL or Media Gateway v VAL announcement circuit pack, it must be properly installed and configured. These instructions are contained in other documents in the Communication Manager documentation library.

- For a complete description of Announcement information and procedures, see the “Announcements” feature in the *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.
- For a complete description of the related Locally Sourced Announcement feature, see the “Locally Sourced Announcements and Music” feature in the *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.
- For more information about these and other tasks related to using the VAL, see the documents listed in the following table.

Task	Information source
Installing the VAL circuit pack Administering IP Connections Adding IP Routes Testing the IP Connections	*Made Easy Tool for DEFINITY Server Configurations Installation, Upgrades and Additions for the Avaya CMC1 Media Gateway*.
Installing v VAL for a Media Gateway using the Media-Gateway screen and the **`enable announcement`** command	Each Media Gateway that will be used to provide announcements through the embedded VAL circuitry on the Gateway processor circuit pack must be assigned on

Task	Information source
Administering IP Connections Adding IP Routes Testing the IP Connections ✱ **Note:** Media Gateway embedded VAL announcements (v VAL) must have the gateway(s) that will provide announcements enabled in order for announcement extensions assigned to that gateway to be played.	the Media-Gateway screen and enabled using the **`enable announcements`** command before announcements can be recorded using the telephone or played from that gateway. ✱ **Note:** For more information about the Media-Gateway screen, and for a description of commands, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300191. Announcements can be administered to a gateway and files can be FTPed to that gateway even though it is not enabled. However, the Media Gateway first must be assigned on the Media-Gateway screen so as to be used for gateway announcements. Each Media Gateway when enabled is counted as a VAL circuit pack towards the system limit of either 1 VAL circuit pack (if the **VAL Maximum Capacity** field is `n`) or 10 circuit packs (for the Avaya S8XXX Servers) if the **VAL Maximum Capacity** field is `y`. First the Media Gateway must have the **V9** field assigned to `gateway-announcements` on the Media-Gateway screen before the Media Gateway embedded VAL (v VAL) can be enabled. Then the Media Gateway embedded VAL is enabled using the **`enable announcement-board gggV9`** command (where ggg is the gateway number assigned on the Media-Gateway screen). The Media Gateway embedded VAL also can be disabled using the **`disable announcement-board ggV9`** command. This removes that gateway from the VAL circuit pack count but announcements already assigned and recorded/FTPed on that circuit pack remain but will not play.
Administering Announcements (recording, copying, deleting, and so on.)	*Avaya Aura™ Communication Manager Feature Description and Implementation*.
Viewing announcement usage measurements (**`list`**	*Avaya Aura™ Communication Manager Reports* and *Avaya Aura™ Communication*

Task	Information source
`measurements announcement` command)	*Manager Feature Description and Implementation*.
Troubleshooting announcements	*Avaya Aura™ Communication Manager Feature Description and Implementation*.
Troubleshooting VAL hardware	*Maintenance Procedures for Avaya Aura™ Communication Manager* for your model(s).

Chapter 17: Managing Group Communications

Voice Paging Over Loudspeakers setup

Use this procedure to allow users to make voice pages over an external loudspeaker system connected to Communication Manager. If you're using an external paging system instead of an auxiliary trunk circuit pack, don't use this procedure. External systems typically connect to a trunk or station port and are not administered through the Loudspeaker Paging screen.

See Loudspeaker Paging in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information on voice paging over loudspeakers.

See Speakerphone paging setup for another way to let users page.

Preparing to set up Voice Paging Over Loudspeakers

Procedure

Verify that your server running Communication Manager has one or more auxiliary trunk circuit packs with enough available ports to support the number of paging zones you define.

Each paging zone requires 1 port. For information on specific circuit packs, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

Setting Up Voice Paging Over Loudspeakers example

About this task

As an example, we will set up voice paging for an office with 5 zones. We'll allow users to page all 5 zones at once, and we'll assign a class of restriction of 1 to all zones.

Procedure

1. Enter `change paging loudspeaker`.
2. In the **Voice Paging Timeout** field, enter `30`.

   This field sets the maximum number of seconds a page can last. In our example, the paging party will be disconnected after 30 seconds.
3. In the **Port** field for **Zone 1**, enter `01C0501`.

   Use this field to assign a port on an auxiliary trunk circuit pack to this zone.
4. In the **Voice Paging — TAC** field enter `301`.

   Use this field to assign the trunk access code users dial to page this zone. You cannot assign the same trunk access code to more than one zone.
5. In the **Voice Paging — COR** field enter `1`.

   Use this field to assign a class of restriction to this zone. You can assign different classes of restriction to different zones.
6. On the **Zone 1** row, enter `Reception area` in the **Location** field.

   Give each zone a descriptive name so you can easily remember the corresponding physical location.
7. Repeat steps 4 through 6 for zones 2 to 5.
8. In the **ALL** row, enter `310` in the **Voice Paging — TAC** field and `1` in the **Voice Paging — COR** field.

   By completing this row, you allow users to page all zones at once. You do not have to assign a port to this row.
9. Select `Enter` to save your changes.

   You can integrate loudspeaker voice paging and call parking. This is called “deluxe paging.” You enable deluxe paging by entering `y` in the **Deluxe Paging and Call Park Timeout to Originator** field on the Feature-Related System Parameters screen. To allow paged users the full benefit of deluxe paging, you should also enter a code in the **Answer Back Access Code** field on the Feature Access Code (FAC) screen if you haven’t already: paged users will dial this code + an extension to retrieve calls parked by deluxe paging.

Loudspeaker Paging troubleshooting

This section lists the known or common problems that users might experience with the Loudspeaker Paging feature.

Problem	Possible cause	Action
Users cannot page.	The attendant has control of the trunk group.	Deactivate attendant control.
Calls to an extension are heard over the loudspeakers.	The extension might have been forwarded to a trunk access code used for paging.	Deactivate call forwarding or change the extension to which calls are forwarded.

User considerations for Voice Paging Over Loudspeakers

Users page by dialing the trunk access code assigned to a zone and speaking into their handset. For your users' convenience, you might also want to consider the following options:

- Add the paging trunk access codes to an abbreviated dialing list and allow users to page using the list.
- Assign individual trunk access codes to Autodial buttons.
- Assign individual trunk access codes to Busy buttons. The status lamp tells the user whether or not the trunk is busy.
- For attendants, you can provide one-button paging access by assigning trunk access codes for paging zones to the Direct Trunk Group Select buttons on the attendant console.

With an appropriate class of restriction, remote callers can also make loudspeaker pages.

When deluxe paging is enabled, if a user with an active call dials the trunk access code for a paging zone the active call is automatically parked.

- Users dial the trunk access code + "#" to page and park an active call on their own extensions.
- Users with console permission can park a call on any extension by dialing the trunk access code + the extension.
- Attendants or users with console permissions can park calls to common shared extensions.
- Parked calls can be retrieved from any telephone. Paged users simply dial the answer back feature access code + the extension where the call is parked.

Chime Paging Over Loudspeakers setup

Use this procedure to allow users to make chime pages over an external loudspeaker system connected to your Avaya S8XXX Server. Users page by dialing a trunk access code and the extension of the person they want to page. The system plays a unique series of chimes assigned to that extension. This feature is also known as Code Calling Access.

To set up chime paging, you fill out the necessary fields on the Loudspeaker Paging screen and then assign chime codes to individual extensions on the Code Calling IDs screen.

See Loudpeaker Paging in*Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information on chime paging over loudspeakers.

See Speakerphone paging setup below for another way to let users page.

Preparing to set up Chime Paging Over Loudspeakers

Procedure

Verify that your server running Communication Manager has one or more auxiliary trunk circuit packs with enough available ports to support the number of paging zones you define.

Each paging zone requires 1 port. For information on specific circuit packs, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

Setting up Chime Paging Over Loudspeakers example

About this task

As an example, we will set up chime paging for a clothing store with 3 zones. We'll allow users to page all zones at once, and we will assign a class of restriction of 1 to all zones.

Procedure

1. Enter `change paging loudspeaker`.
2. In the **Code Calling Playing Cycles** field, enter `2`.

   This field sets the number of times a chime code plays when someone places a page.
3. In the **Port** field for **Zone 1**, enter `01A0301`.

   Use this field to assign a port on an auxiliary trunk circuit pack to this zone.
4. In the **Code Calling — TAC** field enter `80`.

   Use this field to assign the trunk access code users dial to page this zone. You cannot assign the same trunk access code to more than one zone.
5. In the **Code Calling — COR** field enter`1`.

Use this field to assign a class of restriction to this zone. You can assign different classes of restriction to different zones.

6. On the **Zone 1** row, enter `Men’s Department` in the **Location** field.

   Give each zone a descriptive name so you can easily remember the corresponding physical location.
7. Repeat steps 4 through 6 for zones 2 and 3.
8. In the **ALL** row, enter`89` in the **Code Calling — TAC** field and `1` in the **Code Calling — COR** field.

   By completing this row, you allow users to page all zones at once. You do not have to assign a port to this row.
9. Select `Enter` to save your changes.

Assigning chime codes example

Procedure

1. Enter **`change paging code-calling-ids`**.
2. Enter the first extension, `2130`, in the **Ext** field for Id 111.

   Each code Id defines a unique series of chimes.
3. Assign chime codes to the remaining extensions by typing an extension number on the line following each code Id.

   You can assign chime codes to as many as 125 extensions.
4. Select `Enter` to save your changes.

Chime Paging Over Loudspeakers troubleshooting

Problem	Possible causes	Solutions
Users report that they can’t page.	The attendant has taken control of the trunk group.	Deactivate attendant control.

User considerations for Chime Paging Over Loudspeakers

Users page by dialing the trunk access code assigned to a zone. For your users' convenience, you might also want to consider the following options:

- Add the paging trunk access codes to an abbreviated dialing list and allow users to page using the list.

  Note:

  Don't use special characters in abbreviated dialing lists used with chime paging.
- Assign individual trunk access codes to Autodial buttons.
- Assign individual trunk access codes to Busy buttons. The status lamp tells the user whether or not the trunk is busy.
- For attendants, you can provide one-button paging access by assigning trunk access codes for paging zones to the **Direct Trunk Group Select** buttons on the attendant console.

With an appropriate class of restriction, remote callers can also make loudspeaker pages.

Speakerphone paging setup

Use this procedure to allow users to make an announcement over a group of digital speakerphones. By dialing a single extension that identifies a group, users can page over all the speakerphones in that group. Speakerphone paging is one-way communication: group members hear the person placing the page but cannot respond directly.

See Group Paging in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information on paging over speakerphones.

Preparing to set up speakerphone paging

Procedure

Verify that you have DCP set speakerphones or IP set speakerphones.

Setting up speakerphone paging example

About this task

To set up speakerphone paging, you create a paging group and assign telephones to it. In the following example, we'll create paging group 1 and add 4 members.

Procedure

1. Enter **`add group-page 1`**.
2. In the **Group Extension** field, enter 3210.

   This field assigns the extension users dial to page the members of this group.
3. In the **Group Name** field, enter `Sales staff`.

   This name appears on callers' telephone displays when they page the group.
4. In the **COR** field, enter `5`.

   Any user who wants to page this group must have permission to call COR 5.
5. In the `Ext` field in row 1, enter `2009`.
6. Enter the remaining extensions that are members of this group.

   Communication Manager fills in the **Name** fields with the names from the Station screen when you save your changes.
7. Set the **Alert** field to y for telephones that require an alert message to enable ringing, for example, Spectralink wireless telephones.
8. Save the changes and exit the screen.

Speakerphone paging troubleshooting

Problem	Possible causes	Solutions
Users get a busy signal when they try to page.	All telephones in the group are busy or off-hook.	Wait a few minutes and try again.
	All telephones in the group have Send All Calls or Do Not Disturb activated.	Group members must deactivate these features in order to hear a page.
Some group members report that they don't hear a page.	Some telephones in the group are busy or off-hook.	Wait a few minutes and try again.

Problem	Possible causes	Solutions
	Some telephones in the group have Send All Calls or Do Not Disturb activated.	Group members must deactivate these features in order to hear a page.

Speakerphone paging capacities

- You can create up to 32 paging groups on Communication Manager.
- Each group can have up to 32 extensions in it.
- One telephone can be a member of several paging groups.

Whisper Paging users who are on active calls

Use this procedure to allow one user to interrupt another user’s call and make a private announcement. This is called whisper paging. The paging user dials a feature access code or presses a feature button, then dials the extension they want to call. All 3 users can hear the tone that signals the page, but only the person on the paged extension can hear the pager’s voice: other parties on the call cannot hear it, and the person making the page cannot hear anyone on the call.

See Whisper Paging in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information on whisper paging.

Preparing to set up Whisper Paging

Procedure

1. Verify that your Communication Manager server has a circuit pack that supports whisper paging.

   For information on specific models, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

2. Verify that your users have 6400-, 7400-, 8400-, or 9400-series DCP (digital) telephones.

Whisper Paging setup

You give users the ability to use whisper paging by administering feature buttons or feature access codes.

You can give users feature buttons that make, answer, or block whisper pages. Using the Station screen, you can administer these buttons in any combination as appropriate:

- Whisper Page Activation — allows this user to place a whisper page
- Answerback — allows this user to answer a whisper page

  Pressing the answerback button automatically puts any active call on hold and connects the paged user to the paging user.
- Whisper Page Off— allows this user to block whisper pages

  If possible, assign this function to a button with a lamp so the user can tell when blocking is active. You cannot administer this button to a soft key.

To allow users to make a whisper page by dialing a feature access code, you simply need to enter a code in the **Whisper Page Activation Access Code** field on the Feature Access Code (FAC) screen. See *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for information about the screens referred in this topic.

Telephones as Intercoms administration

Use this feature to make communications quicker and easier for users who frequently call each other. With the intercom feature, you can allow one user to call another user in a predefined group just by pressing a couple of buttons. You can even administer a button that always calls a predefined extension when pressed.

Administering the intercom feature is a 2-step process. First, you create an intercom group and assign extensions to it. Then, to allow group members to make intercom calls to each other, you administer feature buttons on their telephones for automatic intercom, dial intercom, or both. This section also provides instructions for allowing one user to pick up another user's intercom calls.

See Abbreviated Dialing in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for information on another way for users to call each other without dialing complete extension numbers.

See Intercom in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information on intercom functions.

Administering intercom feature buttons example

About this task

To allow users to make intercom calls, you must administer feature buttons on the telephones in the intercom group. You can administer buttons for dial intercom, automatic intercom, or both on multi-appearance telephones. You can't administer either intercom feature on single-line telephones, but you can assign single-line telephones to intercom groups so those users can receive intercom calls.

As an example, we will set up automatic intercom between extensions 2010 (dial code = 1) and 2011 (dial code = 2) in intercom group 1.

Procedure

1. Enter **`change station 2010`**.
2. Move to the page with the **BUTTON ASSIGNMENTS** fields.
3. In **BUTTON ASSIGNMENTS** field 4, enter `auto-icom`.

   Press `Tab`.

   The **Grp** and **DC** fields appear.
4. In the **Grp** field, enter `1`.

   This is the number of the intercom group. Since an extension can belong to more than one intercom group, you must assign a group number to intercom buttons.
5. In the **DC** field, enter `2`.

   This is the dial code for extension 2011, the destination extension.
6. Select `Enter` to save your changes.
7. Repeat steps 1 to 6 for extension 2011.
   Assign a dial code of 1 to 2011's automatic intercom button.

   To give a member of a group the ability to make intercom calls to all the other members, administer a Dial Intercom button on the member's telephone. Type the number of the intercom group in the **Grp** field beside the **Dial Intercom** button.

   You can also give one user instant, one-way access to another. For example, to give user A instant, one-way access to user B, administer an **Automatic Intercom** button on A's telephone only. You don't have to administer any intercom button on B's telephone. If B has a Dial Intercom button, he can make an intercom call to A the same way as he would to any other group member.

   When users are in the same call pickup group, or if Directed Call Pickup is enabled on your server running Communication Manager, one user can answer an intercom call to another user. To allow users to pick up intercom calls to other users, you must enter `y` in the **Call Pickup on Intercom Calls** field on the Feature-Related System Parameters screen.

Administering an intercom group example

About this task

In this example, we'll create intercom group 1 and add extensions 2010 to 2014

Procedure

1. Enter `add intercom-group 1`
2. Enter `1` in the **Length of Dial Code** field.

   Dial codes can be 1 or 2 digits long.
3. On row 1, enter `2010` in the **Ext** field.
4. On row 1, enter `1` in the **DC** field.

   This is the code a user will dial to make an intercom call to extension 2010. The length of this code must exactly match the entry in the **Length of Dial Code** field.
5. Repeat steps 3 and 4 for the remaining extensions.

   Dial codes don't have to be in order. Communication Manager fills in the **Name** field with the name from the Station screen when you save changes.
6. Select `Enter` to save your changes.

Automatic Answer Intercom Calls setup

About this task

Automatic Answer Intercom Calls (Auto Answer ICOM) allows a user to answer an intercom call within the intercom group without pressing the intercom button. Auto Answer ICOM works with digital, BRI, and hybrid telephones with built-in speaker, headphones, or adjunct speakerphone.

> **Security alert:**
>
> Press the **Do Not Disturb** button or the **Send All Calls** button on your telephone when you don't want someone in your intercom group to listen in on a call. Auto Answer ICOM does not work when the **Do Not Disturb** button or the **Send All Calls** button is pressed on the telephone.

Administering Auto Answer ICOM example

About this task

This section contains an example, with step-by-step instructions, on how to set up Auto Answer ICOM.

In this example, you set up Auto Answer ICOM on station 12345.

Procedure

1. Enter `change station 12345`.

   The system displays the Station screen for extension 12345. Click **Next Page** until you see the Feature Options page.
2. Move to the **Auto Answer** field and enter `icom`.
3. Select `Enter` to save your changes.

Service Observing Calls

About this task

Use this procedure to allow designated users, normally supervisors, to listen to other users' calls. This capability is often used to monitor service quality in call centers and other environments where employees serve customers over the telephone. On Communication Manager, this is called "service observing" and the user observing calls is the "observer."

This section describes service observing in environments without Automatic Call Distribution (ACD) or call vectoring. To use service observing in those environments, see *Avaya Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568.

See Service Observing in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 55-245-205, for detailed information on service observing.

Preparing to set up Service Observing

1. On the System Parameter Customer-Options screen, verify that the:
   - **Service Observing (Basic)** field is `y`.
2. If you want to enable remote service observing by allowing remote users to dial a feature access code, verify the:
   - **Service Observing (Remote/By FAC)** field is `y`.

If the appropriate field is not enabled, contact your Avaya representative.

Setting up Service Observing example

About this task

Security alert:

Listening to someone else's calls might be subject to federal, state, or local laws, rules, or regulations. It might require the consent of one or both of the parties on the call. Familiarize yourself with all applicable laws, rules, and regulations and comply with them when you use this feature.

In this example, we'll set up service observing for a manager. The manager's class of restriction is 5. We'll assign a feature button to the manager's telephone and allow her to monitor calls on local extensions that have a class of restriction of 10. Everyone on an observed call will hear a repetitive warning tone.

Procedure

1. Set the observer's class of restriction to permit service observing:
   a. In the Class of Restriction screen for COR 5, enter `y` in the **Can Be A Service Observer** field.
   b. Move to the page of the Class of Restriction screen that shows service observing permissions.
   c. Enter `y` in the field for class of restriction 10.
2. In the Class of Restriction screen for COR 10, enter `y` in the **Can Be Service Observed** field.

   Anyone with class of restriction 5 now has permission to observe extensions with class of restriction 10. To further restrict who can observe calls or be observed, you might want to create special classes of restriction for both groups and use these classes only for the appropriate extensions.
3. In the Station screen, assign a **Service Observing** button to the observer's telephone.

A service observing button permits users to switch between listen-only and listen-and-talk modes simply by pressing the button.

4. To activate the warning tone, enter `y` in the **Service Observing — Warning Tone** field on the Feature-Related System Parameters screen.

   A unique 2-second, 440-Hz warning tone plays before an observer connects to the call. While the call is observed, a shorter version of this tone repeats every 12 seconds.

5. For users to activate service observing by feature access codes, use the Feature Access Code (FAC) screen to administer codes in one or both of the following fields:

   - **Service Observing Listen Only Access Code**
   - **Service Observing Listen/Talk Access Code**

     When using feature access codes, observers must choose a mode at the start of the session. They cannot switch to the other mode without ending the session and beginning another.

   Note:

   Feature access codes are required for remote observing.

Best practices for service observing

Procedure

1. Do not add a bridged appearance as line appearance 1 for any station.

   Doing this can cause unexpected feature interactions with features like Service Observing and TTI.

2. You can observe calls on a primary extension as well as all bridged appearances of that extension.

   You cannot observe the bridged appearances on the bridged extension's telephone. For example, if you are observing extension 3082 and this telephone also has a bridged appearance for extension 3282, you cannot observe calls on the bridged call appearance for 3282. But if you observe extension 3282, you can observe activity on the primary and all of the bridged call appearances of 3282.

3. If you are a primary telephone user or a bridging user, you can bridge onto a service observed call of the primary at any time.

   If you are a bridging user, you cannot activate Service Observing using a bridged call appearance.

4. If the primary line is service observing on an active call, a bridged call appearance cannot bridge onto the primary line that is doing the service observing.

Chapter 18: Managing Data Calls

Types of Data Connections

You can use Communication Manager to allow the following types of data elements/devices to communicate to the world:

- Data Terminals
- Personal computers
- Host Computers (for example, CentreVu CMS or Communication Manager Messaging)
- Digital Phones (Digital Communications Protocol (DCP) and Integrated Services Digital Network-Basic Rate Interface (ISDN-BRI))
- Audio/Video Equipment
- Printers
- Local area networks (LAN)

You enable these connections using a large variety of data communications equipment, such as:

- Modems
- Data Modules
- Asynchronous Data Units (ADU)
- Modem Pools
- Data/modem pooling circuit packs

Once you have connected these data devices to Communication Manager, you can use networking and routing capabilities to allow them to communicate with other devices over your private network or the public network.

This section describes the system features available to enable data communications.

Data Call Setup

Data Call Setup provides multiple methods to set up a data call:

- Data-terminal (keyboard) dialing
- Telephone dialing
- Hayes AT command dialing
- Administered connections
- Hotline dialing

Data Call Setup Administration

Administering Data Call Setup for data-terminal dialing

Procedure

1. Choose one of the following data modules and administer all fields:
   - Processor/Trunk Data Module
   - Data Line Data Module
   - 7500 Data Module
2. On the Modem Pool Group screen, administer the **Circuit Pack Assignments** field.

Administering Data Call Setup for telephone dialing

Procedure

1. Choose one of the following:
   - On the Feature Access Code (FAC) screen, administer the **Data Origination Access Code** field. See Feature Access Code (FAC) in *Avaya Aura™ Communication ManagerScreen Reference*, 03-602878, for more information.
   - On the Station screen, assign one button as data-ext (Ext:).
2. Choose one of the following data modules and administer all fields:

- Processor/Trunk Data Module
- Data Line Data Module

3. On the Modem Pool Group screen, administer the **Circuit Pack Assignments** field.

Data Call Setup port assignments

Depending on the hardware used, assign ports to the following:

- Data modules
- 7400D-series or CALLMASTER digital telephones
- 7500D-series telephones with asynchronous data module (ADM)
- Analog modems (port is assigned using 2500 telephone screen)

Characters used in Data Call Setup

Basic-digit dialing is provided through an ADM or 7500B data module. The user can enter digits from 0 to 9, *, and # from a 7500 or 8500 series telephone keypad or an EIA-terminal interface. In addition, the user can dial the following special characters.

Table 4: Special characters

Character	Use
SPACE, -, (, and)	improves legibility. Communication Manager ignores these characters during dialing.
+ character (wait)	interrupts or suspends dialing until the user receives dial tone
, (pause)	inserts a 1.5-second pause
% (mark)	indicates digits for end-to-end signaling (touch-tone). This is required when the trunk is rotary. It is not required when the trunk is touch-tone.
UNDERLINE or **BACKSPACE**	corrects previously typed characters on the same line
@	deletes the entire line and starts over with a new DIAL: prompt

Each line of dialing information can contain up to 42 characters (the + and % characters count as two each).

Examples of dialing are:

- DIAL: 3478
- DIAL: 9+(201) 555-1212
- DIAL: 8, 555-2368
- DIAL: 9+555-2368+%9999+123 (remote access)

DCP and ISDN-BRI module call-progress messages

The following call-progress messages and their meanings are provided for DCP and ISDN-BRI modules.

Table 5: Call-progress messages

Message	Application	Meaning
DIAL:	DCP	Equivalent to dial tone. Enter the desired number or FAC followed by Enter.
CMD	BRI	Equivalent to dial tone. Enter the desired number or FAC followed by Enter.
RINGING	DCP, BRI	Equivalent to ringing tone. Called terminal is ringing.
BUSY	DCP, BRI	Equivalent to busy tone. Called number is busy or out of service.
ANSWERED	DCP, BRI	Call is answered.
ANSWERED - NOT DATA	DCP	Call is answered and a modem answer tone is not detected.
TRY AGAIN	DCP, BRI	Equivalent to reorder tone. System facilities are currently not available.
DENIED	DCP, BRI	Equivalent to intercept tone. Call cannot be placed as dialed.
ABANDONED	DCP, BRI	Calling user has abandoned the call.
NO TONE	DCP, BRI	Tone is not detected.
CHECK OPTIONS	DCP, BRI	Data-module options are incompatible.
XX IN QUEUE	DCP, BRI	Current position in queue.
PROCESSING	DCP, BRI	Out of queue. Facility is available.
TIMEOUT	DCP, BRI	Time is exceeded. Call terminates.
FORWARDED	DCP, BRI	Equivalent to redirection-notification signal. Called terminal activates Call Forwarding and receives a call, and call is forwarded.

Message	Application	Meaning
INCOMING CALL	DCP, BRI	Equivalent to ringing.
INVALID ADDRESS	DCP	Entered name is not in alphanumeric-dialing table.
WRONG ADDRESS	BRI	Entered name is not in alphanumeric-dialing table.
PLEASE ANS-	DCP, BRI	Originating telephone user transferred call to data module using One-Button Transfer to Data.
TRANSFER	DCP	Data Call Return-to-Voice is occurring.
CONFIRMED	DCP, BRI	Equivalent to confirmation tone. Feature request is accepted, or call has gone to a local coverage point.
OTHER END	DCP, BRI	Endpoint has terminated call.
DISCONNECTED	DCP, BRI	Call is disconnected.
WAIT	DCP, BRI	Normal processing continues.
WAIT, XX IN QUEUE	DCP	Call is in a local hunt-group queue.

DCP data modules

Using DCP data-terminal dialing

About this task

DCP data-terminal dialing allows a user to set up and disconnect data calls directly from a data terminal as follows.

Procedure

1. At the **DIAL** prompt, the user types the data number.
2. If the call is queued, the message **WAIT, XX IN QUEUE** displays.

   The queue position XX updates as the call moves up in queue.
3. To originate and disconnect a call, the user presses **BREAK**.

   If the terminal does not generate a 2-second continuous break signal, the user can press originate/disconnect on the data module.
4. The user can enter digits at the **DIAL**: prompt.

DCP telephone dialing

DCP telephone dialing allows telephone users to originate and control data calls from a telephone.

Users can set up a call using any unrestricted telephone and then transfer the call to a data endpoint.

The primary way to make data calls is with multiappearance telephone data-extension buttons. Assign any administrable feature button as a data-extension button. The data-extension button provides one-touch access to a data module. The number of assigned data-extension buttons per telephone is not limited.

The following options, either alone or combined, permit flexibility in making data calls from a telephone.

- One-Button Transfer to Data

  A user can transfer a call to the associated data module by pressing the data-extension button after the endpoint answers.

- Return-to-Voice

  A user can change the connection from data to voice. The user presses the data-extension button associated with the busy data module. If the user hangs up, the call disconnects. Return of a data call to the telephone implies that the same data call is continued in the voice mode, or transferred to point.

  The Return-to-Voice feature is denied for analog adjuncts.

- Data Call Preindication

  A user, before dialing a data endpoint, can reserve the associated data module by pressing the data-extension button. This ensures that a conversion resource, if needed, and the data module are reserved for the call. Avaya recommends the use of Data Call Preindication before 1-button transfer to data for data calls that use toll-network facilities. Data Call Preindication is in effect until the associated data-extension button is pressed again for a 1-button transfer; there is no time-out.

ISDN-BRI data modules

Using ISDN-BRI data-terminal dialing

About this task

Your can set up and disconnect data calls directly from a data terminal without using a telephone as follows:

Procedure

1. Press `Enter` a few times.
2. If the CMD: prompt does not appear, press **Break A + T** at the same time, and then press `Enter`..
3. At the **CMD**: prompt, the user types and presses au `Enter`.
4. To disconnect, enter +++.
5. At the CMD: prompt, the type end and press `Enter`.

ISDN-BRI telephone dialing

To make a data call, an ISDN-BRI telephone user presses the data button on the terminal, enters the number on the dial pad, and then presses the data button again.

The following data functions are not available on ISDN-BRI telephones:

- One-Button Transfer to Data
- Return-to-Voice
- Data Call Preindication
- Voice-Call Transfer to Data and Data-Call Transfer to Voice

The system handles all presently defined BRI bearer data-call requests. Some capabilities that are not supported by Avaya terminals are provided by non-Avaya terminals. If Communication Manager does not support a capability, a proper cause value returns to the terminal.

BRI terminals receive a cause or reason code that identifies why a call is being cleared. The BRI data module converts certain cause values to text messages for display.

In a passive-bus multipoint configuration, the system supports two BRI endpoints per port, thus doubling the capacity of the BRI circuit pack. When you change the configuration of a BRI from point-to-point to multipoint, the original endpoint does not need to reinitialize. Only endpoints that support service profile identifier (SPID) initialization can be administered in a multipoint configuration.

Analog modems

When a telephone user places a data call with a modem, the user dials the data-origination access code assigned in the system before dialing the endpoint.

Considerations for Data Call Setup

- A BRI telephone cannot call a data terminal, and a data terminal cannot call a BRI telephone.

Interactions for Data Call Setup

- Abbreviated Dialing

  Only 22 of the 24 (maximum) digits in an abbreviated-dialing number are available for keyboard dialing. The remaining two digits must contain the wait indicator for tone detection.

- Call Coverage

  A hunt group made up of data endpoints cannot be assigned a coverage path.

- Call Detail Recording

  CDR records the use of modem pools on trunk calls.

- Call Forwarding All Calls

  Calls received by a data module can be forwarded. Activate Call Forwarding All Calls with data-terminal (keyboard) dialing. If the forwarded-to endpoint is an analog endpoint and the caller is a digital endpoint, modem pooling is activated automatically.

- Pooled Modems with Hunt Groups

  UCD can provide a group of data modules or analog modems for answering calls to connected facilities (for example, computer ports).

- World-Class Tone Detection

  Multiple-line data-terminal dialing is supported if the administered level of tone detection is precise. You can administer tone-detection options. The message that Data Call Setup sends to users varies according to the option.

  If the option is not set to precise, and a data call is set up over an analog trunk, messages describing the status of the called endpoint (for example, RINGING, BUSY, TRY AGAIN) change according to which tone-detection option is selected.

Alphanumeric Dialing

Alphanumeric Dialing enhances data-terminal dialing by allowing users to place data calls by entering an alphanumeric name rather than a long string of numbers.

For example, a user could type 9+1-800-telefon instead of 9+1-800-835-3366 to make a call. Users need to remember only the alpha-name of the far-end terminating point.

Alphanumeric Dialing allows you to change a mapped string (digit-dialing address) without having to inform all users of a changed dial address. Users dial the alpha name.

When a user enters an alphanumeric name, the system converts the name to a sequence of digits according to an alphanumeric-dialing table. If the entered name is not found in the table, the system denies the call attempt and the user receives either an `Invalid Address` message (DCP) or a `Wrong Address` message (ISDN-BRI).

Because data terminals access Communication Manager via DCP or ISDN-BRI data modules, dialing procedures vary:

- For DCP, at the `DIAL`: prompt users type the alphanumeric name. Press `Enter`.
- For ISDN-BRI, at the **`CMD`**:prompt users type `d`, a space, and the alphanumeric name. Press `Enter`.

More than one alphanumeric name can see the same digit string.

Administering Alphanumeric Dialing

Procedure

On the Alphanumeric Dialing Table screen, administer the **Alpha-name** and **Mapped String** fields.

Considerations for Alphanumeric Dialing

Note:

Alphanumeric dialing does not apply to endpoints with Hayes modems.

Data Hotline

Data Hotline provides for automatic-nondial placement of a data call preassigned to an endpoint when the originating server goes off-hook. Use for security purposes.

If endpoint software allows users to select the dial function without entering a number, the endpoint can be used for hotline dialing.

Administering Data Hotline

About this task

You can use an abbreviated dialing list for your default ID. See Abbreviated Dialing in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information.

Procedure

1. On the Station screen, administer the following fields.
   - **Abbreviated Dialing List**
   - **Special Dialing Option**
   - **Hot Line Destination**
2. On the Data Module screen, administer the **Abbreviated Dialing List1** field.

   The system automatically places Data Hotline calls to preassigned extensions or off-premises numbers. Calling terminals are connected to the system by a data module. Users should store the destination number in the abbreviated dialing list for future reference.

Interactions for Data Hotline

- Call Forwarding — All Calls

A Data Hotline caller cannot activate both Call Forwarding and Data Hotline. Dialing the Call Forwarding feature access code (FAC) causes activation of the Data Hotline instead.

Data Privacy

Data Privacy protects analog data calls from being disturbed by any of the system's overriding or ringing features.

Administering Data Privacy

Procedure

1. Choose either of the following:
    - On the Feature Access Code (FAC) screen, administer the **Data Privacy Access Code** field.
    - On the Class of Service screen, administer the **Data Privacy** field.
2. On the Station screen, administer the **Class of Service** field.

    To activate this feature, the user dials the activation code at the beginning of the call.

Considerations for Data Privacy

- Data Privacy applies to both voice and data calls. You can activate Data Privacy on Remote Access calls, but not on other incoming trunk calls. Data Privacy is canceled if a user transfers a call, is added to a conference call, is bridged onto a call, or disconnects from a call. You can activate Data Privacy on calls originated from attendant consoles.
- For virtual extensions, assign the Data Privacy Class of Service to the mapped-to physical extension.

Interactions for Data Privacy

- Attendant Call Waiting and Call Waiting Termination

    If Data Privacy is active, Call Waiting is denied.
- Bridged Call Appearance — Single-Line Telephone

If you activate Data Privacy or assign Data Restriction to a station involved in a bridged call and the primary terminal or bridging user attempts to bridge onto the call, this action overrides Data Privacy and Data Restriction.

- Busy Verification

  Busy Verification cannot be active when Data Privacy is active.

- Intercom — Automatic and Dial

  An extension with Data Privacy or Data Restriction active cannot originate an intercom call. The user receives an intercept tone.

- Music-on-Hold Access

  If a user places a call with Data Privacy on hold, the user must withhold Music-on-Hold to prevent the transmission of tones that a connected data service might falsely interpret as a data transmission.

- Priority Calls

  If a user activates Data Privacy, Priority Calls are denied on analog telephones. However, Priority Calls appear on the next available line appearance on multiappearance telephones.

Default Dialing

Default Dialing provides data-terminal users who dial a specific number the majority of the time a very simple method of dialing that number. Normal data terminal dialing and alphanumeric dialing are unaffected.

Default Dialing enhances data terminal (keyboard) dialing by allowing a data-terminal user to place a data call to a preadministered destination by either pressing `Enter` at the DIAL: prompt (for data terminals using DCP data modules) or typing `d` and pressing `Enter` at the CMD: prompt (for data terminals using ISDN-BRI data modules). The data-terminal user with a DCP data module can place calls to other destinations by entering the complete address after the DIAL: prompt (normal data terminal dialing or alphanumeric dialing). The data-terminal user with an ISDN-BRI data module can place calls to other destinations by typing `d`, a space, the complete address. Press `Enter` after the CMD: prompt.

Note:

DU-type hunt groups connecting the system to a terminal server on a host computer have hunt-group extensions set to `no` keyboard dialing.

For the AT command interface supported by the 7400A/7400B/8400B data module, to dial the default destination, enter the ATD command (rather than press return).

Administering Default Dialing

About this task

You can use an abbreviated dialing list for your default ID. See Abbreviated Dialing in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information.

Procedure

On the Data Module screen, administer the following fields:

- **Special Dialing Option** as default.
- **Abbreviated Dialing List**, enter the list to use.
- **AD Dial Code**.

Data Restriction

Data Restriction protects analog-data calls from being disturbed by any of the system's overriding or ringing features or system-generated tones.

Data Restriction applies to both voice and data calls.

Once you administer Data Restriction for an analog or multiappearance telephone or trunk group, the feature is active on all calls to or from the terminal or trunk group.

Note:

Do not assign Data Restriction to attendant consoles.

Administering Data Restriction

Procedure

1. On the Station screen, set the **Data Restriction** field to .
2. Choose one of the following trunk groups and set the **Data Restriction** field to `y` ou.
   - Access
   - Advanced Private-Line Termination (APLT)

- Circuit Pack (CP)
- Customer-Premises Equipment (CPE)
- Direct Inward Dialing (DID)
- Foreign Exchange (FX)
- Integrated Services Digital Network-Primary Rate Interface (ISDN-PRI)
- Release-Link Trunk (RLT)
- Tandem
- Tie
- Wide Area Telecommunications Service (WATS)

Interactions for Data Restriction

- Attendant Call Waiting and Call Waiting Termination

  If Data Restriction is active, Call Waiting is denied.
- Busy Verification

  Busy Verification cannot be active when Data Restriction is active.
- Intercom — Automatic and Dial

  An extension with Data Privacy or Data Restriction activated cannot originate an intercom call. The user receives an Intercept tone.
- Music-on-Hold Access

  If a user places a call with Data Restriction on hold, The user must withhold Music-on-Hold to prevent the transmission of tones that a connected data service might falsely interpret as a data transmission.
- Priority Calls

  Priority Calls are allowed if the analog station is idle. Call Waiting (including Priority Call Waiting) is denied if the station is busy. However, Priority Calls appear on the next available line appearance on multiappearance telephones.
- Service Observing

  A data-restricted call cannot be service observed.

Data-Only Off-Premises Extensions

Data-Only Off-Premises Extensions allows users to make data calls involving data communications equipment (DCE) or digital terminal equipment (DTE) located remotely from the system site.

A Data-Only Off-Premises Extension uses an on-premises modular trunk data module (MTDM). The system communicates with remote data equipment through the private-line facility linking the on-premises MTDM and the remote data equipment.

Users can place data calls to this type of data endpoint using Telephone Dialing or Data Terminal (Keyboard) Dialing. Since there is no telephone at the remote site, originate data calls from the remote data terminal using Keyboard Dialing only.

Administering Data-Only Off-Premises Extensions

Procedure

On the Processor/Trunk Data Module screen, administer all fields.

See Data Module in *Avaya Aura™ Communication Manager Screen Reference* 03-602878, for more information.

Considerations for Data-Only Off-Premises Extensions

The system does not support communications between two TDMs. Modem Pooling is similar to a TDM, it cannot be used on calls to or from a Data-Only Off-Premises Extension.

Interactions for Data-Only Off-Premises Extensions

- Telephone Dialing

  An on-premises multiappearance telephone might have a Data Extension button associated with the TDM used for a Data-Only Off-Premises Extension. The telephone user and the remote user share control of the data module. Actions of the user at the telephone might affect the remote user.

  - 1-Button Transfer to Data

The telephone user can transfer a call to the Data-Only Off-Premises Extension. The Data Extension button lamp on the telephone lights and the Call in Progress lamp on the data module lights during a data call.

- Data Call Preindication

  The multiappearance telephone user presses the idle associated Data Extension button to reserve a data module. The data module is busy to all other users. When the user reserves a data module, the lamp associated with the Data Extension button winks and lights at any other associated telephones. A remote user receives the BUSY message when attempting to originate a call.

- Return-to-Voice

  To establish a data call, the telephone user presses the associated busy Data Extension button to transfer the call to the telephone. The data module associated with the Data Extension button is disconnected from the call. The Call in Progress lamp on the data module goes dark.

Data Modules — General

A data module is a connection device between a basic-rate interface (BRI) or DCP interface of the Avaya S8XXX Server and DTE or DCE.

The following types of data modules can be used with the system:

- Announcement data module
- Data line data module
- Processor/trunk data module (P/TDM)
- 7500 data module
- World Class BRI data module
- Ethernet data module.
- Point-to-Point Protocol (PPP) data module.

For more information, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

Note:

The 51X series Business Communications Terminals (BCT) are not administered on the Data Module screen. The 510 BCT (equivalent to a 7405D with a display and built-in DTDM), 515 BCT (equivalent to a 7403D integrated with 7405D display module function, data terminal and built-in DTDM), and the 7505D, 7506D, and 7507D have a DCP interface but have built-in data module functionality. Both are administered by means of the Station screen in Communication Manager.

Detailed description of data modules

TTI allows data modules without hardware translation to merge with an appropriate data module connected to an unadministered port. The unadministered port is given TTI default translation sufficient to allow a terminal connected to the data module (connected to the port) to request a TTI merge with the extension of a data module administered without hardware translation.

Note:

TTI is not useful for Announcement and X.25 hardware.

Administration Without Hardware supports PDM, TDM, Data-Line, Announcement, and X.25 data modules.

Note:

The 513 BCT has an EIA interface rather than a DCP interface (no built in data module, attachable telephone, or telephone features). The 513 BCT is not administered; only the data module to which the 513 BCT is connected is administered.

7400A/7400B+/8400B+ Data Module

Use the 7400A data module instead of an MTDM when you support combined Modem Pooling. The 7400A data module supports asynchronous operation at speeds up to 19200-bps, and provides a DCP interface to the server and an EIA 232C interface to the associated modem. The 7400A operates in stand-alone mode as a data module.

7400B+ and 8400B+ data modules support asynchronous-data communications and operate in stand-alone mode for data-only service or in linked mode, which provides simultaneous voice and data service. The 7400B+ and 8400B+ provide voice and data communications to 7400D series telephones and 602A1 CALLMASTER telephones that have a connection to a data terminal or personal computer. The data modules integrate data and voice into the DCP protocol required to interface with the server via a port on a digital-line circuit pack. Use the 7400B+ or 8400B+ instead of an MPDM when you need asynchronous operation at speeds up to 19.2-kbps to provide a DCP interface to the server for data terminals and printers. The 7400B+ and 8400B+ do not support synchronous operation and keyboard dialing. Dialing is provided using the standard Hayes command set.

7400D

This data module supports synchronous operation with Communication Manager Messaging, CMS, and DCS. It provides synchronous data transmissions at speeds of 19.2-Kbps full duplex.

7400C High Speed Link

The 7400C high-speed link (HSL) is a data-service unit that allows access to DCP data services. It provides synchronous data transmission at speeds of 56- and 64-Kbps and provides a link to high-speed data networks. Used for Group 4 fax applications that include electronic mail and messaging, and electronic storage of printed documents and graphics. Use the 7400C for video teleconferencing and LAN interconnect applications.

7500 Data Modules

The 7500 Data Module connects DTE or DCE to the ISDN network. The 7500 Data Module supports EIA 232C and V.35 interfaces and RS-366 automatic-calling unit interface (for the EIA 232C interface only).

The 7500 has no voice functions. Configure in the following ways:

- Asynchronous DCE

  300, 1200, 2400, 4800, 9600, 19200-bps
- Synchronous DCE

  1200, 2400, 4800, 9600, 19200, 56000, 64000-bps
- Asynchronous DTE (used for modem pooling)

  up to 19200-bps

The 7500 Data Module is stand-alone or in a multiple-mount housing.

Asynchronous Data Module

Note:

The **`alias station`** command cannot be used to alias data modules.

Use the Asynchronous Data Module (ADM) with asynchronous DTEs as a data stand for the 7500 and 8500 Series of ISDN-BRI telephones, thus providing connection to the ISDN network. The ADM provides integrated voice and data on the same telephone and supports data rates of 300, 1200, 2400, 4800, 9600, and 19200-bps. This module also supports the Hayes command set, providing compatibility with PC communications packages.

Administered Connections

Use the Administered Connections (AC) feature to establish an end-to-end connection between two access or data endpoints. Communication Manager automatically establishes the connection based on the attributes that you administer. The Administered Connections feature provides the following abilities:

- Support of both permanent and scheduled connections
- Autorestoration (preserving the active session) for connections that are routed over Software Defined Data Network (SDDN) trunks
- An administrable retry interval from 1 to 60 minutes for each AC
- An administrable alarm strategy for each AC
- An establish, retry, autorestoration order that is based on administered priority

Detailed description of Administered Connections

Establish an AC between the following:

- Two endpoints on the same Avaya DEFINITY server or Avaya S8XXX Server
- Two endpoints in the same private network, but on different servers
- One endpoint on the controlling server and another endpoint off the private network

In all configurations, administer the AC on the server having the originating endpoint. For an AC in a private network, if the two endpoints are on two different servers, normally the connection routes via Automatic Alternate Routing (AAR) through tie trunks (ISDN, DS1, or analog tie trunks) and intermediate servers. If required, route the connection via Automatic Route Selection (ARS) and Generalized Route Selection (GRS) through the public network. The call routes over associated ISDN trunks. When the far-end answers, a connection occurs between the far-end and the near-end extension in the `Originator` field on the Administered Connection screen.

Because the system makes an administered connection automatically, you do not use the following:

- Data Call Setup

  Do not assign a default dialing destination to a data module when it is used in an AC.
- Data Hotline

  Do not assign a hotline destination to a data module that is used in an AC.
- Terminal Dialing

  Turn off terminal dialing for data modules involved in an AC. This prevents display of call-processing messages (INCOMING CALL,...) on the terminal.

Access endpoints used for Administered Connections

Access endpoints are nonsignaling trunk ports. Access endpoints neither generate signaling to the far-end of the trunk nor respond to signaling from the far-end. You designate an access endpoint as the originating endpoint or the destination endpoint in an AC.

Typical applications for Administered Connections

The following examples are typical AC applications:

- A local data endpoint that connects to a local or a remote access endpoint, such as:
    - A modular processor data model (MPDM) ACCUNET digital service that connects to SDDN over an ISDN trunk-group DS1 port; an MPDM
    - An MPDM ACCUNET digital service that connects to an ACCUNET Switched 56 Service over a DS1 port
- A local-access endpoint that connects to a local or a remote access endpoint, such as a DSO cross-connect and a 4-wire leased-line modem to a 4-wire modem connection over an analog tie trunk
- A local data endpoint that connects to a local or a remote data endpoint such as a connection between two 3270 data modules

Conditions for establishing Administered Connections

The originating server attempts to establish an AC only if one of the following conditions exist:

- AC is active.
- AC is due to be active. That is, the AC is a permanent AC, or it is the administered time-of-day for a scheduled AC.
- The originating endpoint is in the in-service or idle state.

If the originating endpoint is not in service or is idle, no activity takes place for the AC until the endpoint transitions to the necessary state. The originating server uses the destination address to route the call to the desired endpoint. When the server establishes two or more ACs at the same time, the server arranges the connections in order of priority.

AC attempts can fail because:

- Resources are unavailable to route to the destination.
- A required conversion resource is unavailable.
- Access is denied by Class of Restriction (COR), facilities restriction level (FRL), Bearer Capability Class (BCC), or an attempt is made to route voice-band data over SDDN trunks in the public switched network.
- The destination address is incorrect.
- The destination endpoint is busy.
- Other network or signaling failures occur.

In the event of a failure, an error is entered into the error log. This error generates an alarm, if your alarming strategy warrants an alarm. You can display AC failures with the **`display status-administered connection`** command. The originating server continues to try to establish an AC as long as an AC is scheduled to be active, unless the attempt fails because of an administrative error (for example, a wrong number) or a service-blocking condition, such as outgoing calls are barred).

- The administered retry interval of 1 to 60 minutes for each AC determines the frequency with which failed attempts are retried.
- Retries are made after the retry interval elapses, regardless of the restorable attribute of the AC.
- ACs are retried in priority order.
- When you change the time of day on the server, an attempt is made to establish all ACs in the waiting-for-retry state.

Conditions for dropping Administered Connections

An AC remains active until one of the following scenarios occurs:

- The AC is changed, disabled, or removed.
- The time-of-day requirements of a scheduled AC are no longer satisfied.
- One of the endpoints drops the connection. An endpoint might drop a connection because of user action (in the case of a data endpoint), maintenance activity that results from an endpoint failure, busying out of the endpoint, or handshake failure. If the endpoints are incompatible, the connection is successful until handshake failure occurs.

Note:

An AC between access endpoints remains connected even if the attached access equipment fails to handshake.

- An interruption, such as a facility failure, occurs between the endpoints. If an AC drops because the AC was disabled, removed, or is no longer due to be active, no action is taken. If an AC drops because of changed AC attributes, the system makes an immediate attempt to establish the connection with the changed attributes, if the AC is still scheduled to be active. Existing entries in the error or alarm log are resolved if the entries no longer apply. If an AC involves at least one data endpoint, and handshake failure causes the connection to be dropped, no action is taken for that AC until you run the **`change administered-connection`** command.

Autorestoration and fast retry

When an active AC drops prematurely, you must invoke either autorestoration or fast retry for autorestoration to be attempted for an active AC. If you administer an AC for autorestoration and the connection was routed over SDDN trunks, auto restoration is attempted. During restoration, connections are maintained between the server and both endpoints. In addition to maintaining the active session, AC also provides a high level of security by prohibiting other connections from intervening in active sessions. Autorestoration is usually complete before the 60-second endpoint holdover interval. If autorestoration is successful, the call might be maintained, but this is not guaranteed. The restoration is transparent to the user, with the exception of a temporary disruption of service while restoration is in progress. A successful restoration is indicated by the restored value in the **Connection State** field on the Administered-Connection Status screen. Although a restoration is successful, the data session might not be preserved.

If autorestoration is not active, or if the AC is not routed over SDDN trunks, the server immediately attempts a fast retry to reestablish the connection. The server also attempts a retry if the originating endpoint caused the drop. With fast retry, connections are not maintained on both ends. Fast retry is not attempted for an AC that was last established with fast retry, unless that AC is active for at least 2 minutes. If autorestoration or fast retry fails to restore or reestablish the connection, the call drops, and the AC goes into retry mode. Retry attempts continue, at the administered retry interval, as long as the AC is scheduled to be active.

Administering Administered Connections

Procedure

1. Choose one of the following data modules and administer all fields:

- Data Line Data Module (use with Data Line circuit pack)
- Processor/Trunk Data Module (use with one of the following:)
    - MPDMs, 700D, 7400B, 7400D, or 8400B
    - MTDMs, 700B, 700C, 700E, or 7400A
- Processor Interface Data Module (for more information, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504)
- 25 Data Module (for more information, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504)
- 7500 Data Module (use with ISDN Line 12-BRI-S-NT or ISDN Line 12-BRI-U-NT circuit pack)
- World Class Core BRI Data Module (use with wcbri)

2. On the DS1 Circuit Pack screen, administer all fields.
   Use with switch node carriers.
3. On the Access Endpoint screen, administer all fields.
4. On the Trunk Group screen, choose one of the following trunk groups and administer all fields.
    - ISDN-BRI
    - ISDN-PRI
    - Tie
5. On the Class of Restriction screen, administer all fields.
6. On the Class of Service screen, administer all fields.
7. On the Dial Plan Parameters screen, administer the **Local Node Number** field with a number from 1-63 that matches the DCS switch node number and the CDR node number.
8. On the Administered Connection screen, administer all fields.
9. On the Station screen, assign one button as ac-alarm.
10. On the Attendant Console screen, assign one button as ac-alarm.

Interactions for Administered Connections

- Abbreviated Dialing

Use Abbreviated Dialing entries in the `Destination` field. Entries must comply with restrictions.

- Busy Verification of Stations and Trunks

  This feature does not apply to access endpoints because they are used only for data.

- Call Detail Recording

  For an AC that uses a trunk when CDR is active, the origination extension is the originator of the call.

- Class of Restriction

  Reserve a COR for AC endpoints and SDDN trunks. This restricts endpoints that are not involved in AC from connecting to SDDN trunks or endpoints involved in AC.

- Class of Service/Call Forwarding

  Assign to an AC endpoint a COS that blocks Call Forwarding activation at the endpoint.

- Digital Multiplexed Interface (DMI)

  Use DMI endpoints as the destination in an AC. DMI endpoints do not have associated extensions, so do not use them as the originator in an AC.

- Facility Test Calls

  The feature does not apply to access endpoints because an access endpoint acts as an endpoint rather than as a trunk.

- Modem Pooling

  If you require a modem in an AC, one is inserted automatically. If no modem is available, the connection is dropped.

- Non-Facility Associated Signaling (NFAS) and D-Channel Backup

  Auto restoration for an AC that is initially routed over an NFAS facility can fail if the only backup route is over the facility on which the backup D-channel is administered. The backup D-channel might not come into service in time to handle the restoration attempt.

- **`Set Time`** Command

  When you change the system time via the **`set time`** command, all scheduled ACs are examined. If the time change causes an active AC to be outside its scheduled period, the AC is dropped. If the time change causes an inactive AC to be within its scheduled period, Communication Manager attempts to establish the AC.

  If any AC (scheduled or continuous) is in retry mode and the system time changes, Communication Manager attempts to establish the AC.

- System Measurements

  Access endpoints are not measured. All other trunks in an AC are measured as usual.

Modem Pooling

Modem Pooling allows switched connections between digital-data endpoints (data modules) and analog-data endpoints via pods of acoustic-coupled modems. The analog-data endpoint is either a trunk or a line circuit.

Data transmission between a digital data endpoint and an analog endpoint requires conversion via a modem, because the DCP format used by the data module is not compatible with the modulated signals of an analog modem. A modem translates DCP format into modulated signals and vice versa.

Modem Pooling feature provides pools of integrated-conversion modems and combined-conversion modems.

Integrated-conversion modem pools have functionality integrated on the Pooled Modem circuit pack, providing two modems. Each one emulates a TDM cabled to a 212 modem. Integrated are modem pools not available in countries that use A-law companding.

Combined-conversion modem pools are TDMs cabled to any TDM-compatible modem. Combined-conversion modem pools can be used with all systems.

The system can detect the needs for a modem. Data calls from an analog-data endpoint require that the user indicate the need for a modem, because the system considers such calls to be voice calls. Users indicate this need by dialing the data-origination access code field on the Feature Access Code (FAC) screen before dialing the digital-data endpoint.

The system provides a Hold Time parameter to specify the maximum time any modem can be held but not used (while a data call is in queue).

Administering Integrated Modem Pooling

Procedure

1. On the Modem Pool Group screen, administer all fields.
2. On the Feature Access Code (FAC) screen, administer the **Data Origination Access Code** field.
3. On the Data Module screen, administer all fields.

Administering Combined Modem Poolings

Procedure

1. On the Modem Pool Group screen, administer all fields.
2. On the Feature Access Code (FAC) screen, administer the **Data Origination Access Code** field.

Considerations for Modem Pooling

- On data calls between a data module and an analog-data endpoint, Return-to-Voice releases the modem and returns it to the pool. The telephone user connects to the analog-data endpoint.
- For traffic purposes, the system accumulates data on modem-pooling calls separate from voice calls. Measurements on the pools also accumulate.
- Modem Pooling is not restricted. Queuing for modems is not provided, although calls queued on a hunt group retain reserved modems.
- Avoid mixing modems from different vendors within a combined pool because such modems might differ in transmission characteristics.
- Each data call that uses Modem Pooling uses four time slots (not just two). As a result, heavy usage of Modem Pooling could affect TDM bus-blocking characteristics.
- Tandem switches or servers do not insert a pooled modem. The originating and terminating servers or switches insert a pooled modem.

PC Interface

The personal computer (PC) Interface consists of the PC/PBX platforms and PC/ISDN Platform product family. These products are used with Communication Manager to provide users of IBM-compatible PCs fully-integrated voice and data workstation capabilities.

Two groups of different configurations are available for PC Interface: group 1 uses DCP and group 2 uses the ISDN-BRI (Basic Rate Interface) protocol.

The group 1 configurations consist of DCP configurations that use a DCP expansion card in the PC to link to the server or Avaya S8XXX Server. Group 1 (shown in DCP PC interface configuration (Group 1) on page 531) uses the following connections:

- The PC Interface card plugs into an expansion slot on the PC. The card has 2 standard 8-pin modular jacks (line and telephone).
- The digital telephone plugs into the telephone jack on the PC Interface card.
- The line jack on the card provides a digital port connection to Avaya DEFINITY servers.
- The distance between the PC Interface card and the PBX should be no more than 1524m for 24-gauge wire or 1219m for 26-gauge wire.

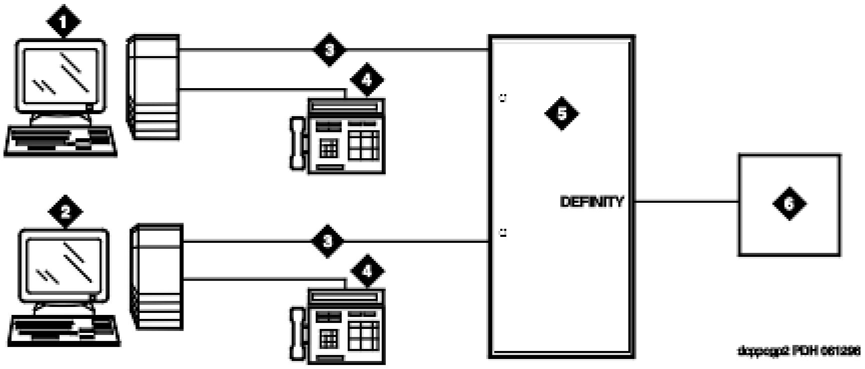


Figure 11: DCP PC interface configuration (Group 1)

Table 6: Figure notes:

a. IBM-compatible PC with DCP Interface card	a. DCP telephone
b. IBM-compatible PC with DCP Interface card	b. Avaya (Digital Line, Digital Line (16-DCP-2-Wire), or Digital Line (24-DCP-2-wire) circuit pack)
c. DCP	c. Host

The group 2 configurations link to the server using a PC/ISDN Interface card installed in the PC. This group can include a stand-alone PC terminal, or up to 4 telephones, handsets, or headsets. Group 2 (shown in the figure on page 532) uses PC/ISDN Interface cards (up to four cards) which plug into expansion slots on the PC. These cards each provide 2 standard 8-pin modular-jack connections for both line connections (to the server or Avaya S8XXX Server) and telephone connections. A standard 4-pin modular jack is also available for use with a handset or headset.

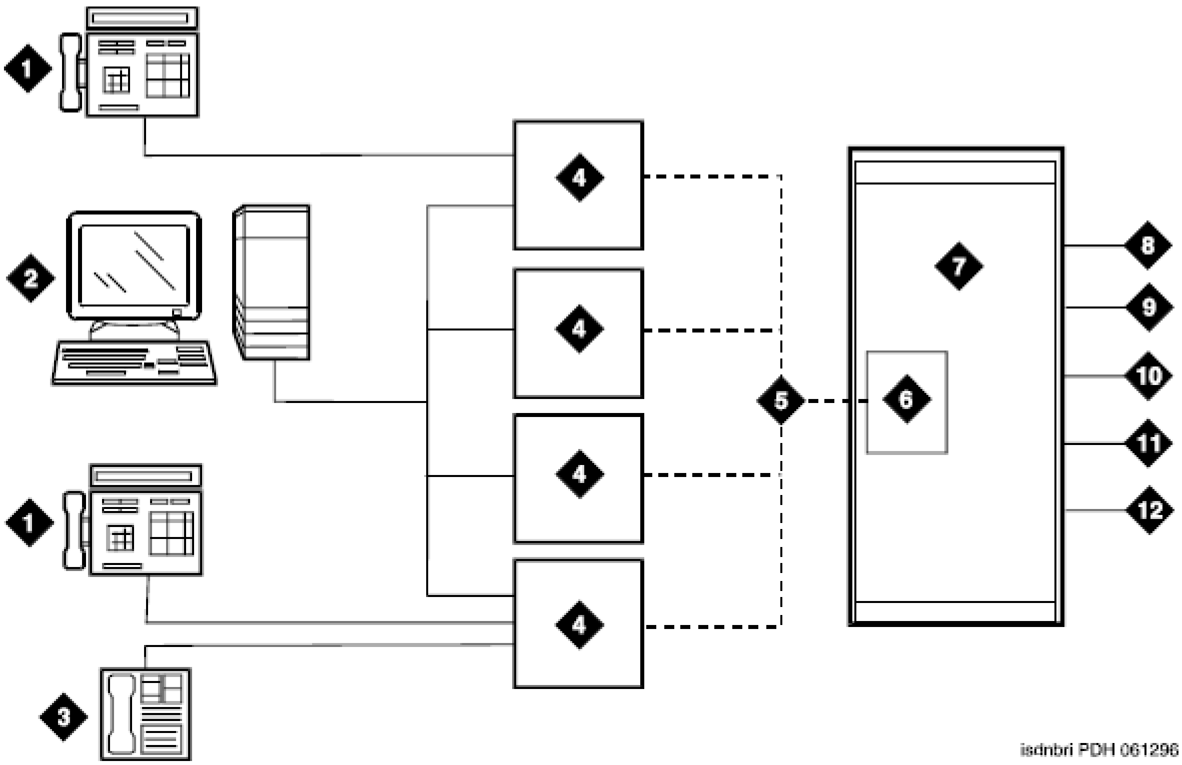


Figure 12: ISDN—BRI PC interface configuration (Group 2)

Table 7: Figure notes:

1. ISDN telephone	1. Avaya S8XXX Server
2. PC with application	2. PRI trunks
3. Handset or Headset	3. BRI stations
4. BRI Interface card	4. Interworking
5. 2B + D	5. DMI
6. ISDN Line (12-BRI-S-NT) circuit pack)	6. Switch features

PC Interface users have multiple appearances (depending on the software application used) for their assigned extension. Designate one or more of these appearances for use with data calls. With the ISDN-BRI version, you can use up to 4 separate PC/ISDN Interface cards on the same PC. Assign each card a separate extension, and assign each extension one or more appearances. The availability of specific features depends on the COS of the extension and the COS for Communication Manager. Modem Pooling is provided to ensure general availability of off-net data-calling services.

PC Interface Security

There are two areas where unauthorized use might occur with this feature: unauthorized local use and remote access.

Security alert:

Unauthorized local use involves unauthorized users who attempt to make calls from a PC. The PC software has a security setting so users can place the PC in Security Mode when it is unattended. You also can assign Automatic Security so that the administration program on the PC is always active and runs in Security Mode. This mode is password-protected.

Security alert:

Remote access involves remote access to the PC over a data extension. Remote users can delete or copy PC files with this feature. You can password-protect this feature. See the *Avaya Toll Fraud and Security Handbook*, 555-025-600, for additional steps to secure your system and to find out about obtaining information regularly about security developments.

Administering a PC interface

Procedure

On the Station screen, set the **Type** field to `pc`.

Considerations for PC Interface

- Use the Function Key Module of the 7405D with PC Interface.
- BRI terminals normally are initializing terminals and require you to assign an SPID. The PC/ISDN Platform (Group 2), in a stand-alone configuration, is a non-initializing BRI terminal and does not require you to assign a SPID.
    - Set a locally-defined terminal type with General Terminal Administration
    - Define the terminal type as a non-initializing terminal that does not support Management Information Messages (MIM).
    - Assign the PC/ISDN Platform with an associated (initializing) ISDN-BRI telephone (such as an ISDN 7505) using a SPID.

  - Assign the station (using a locally-defined terminal type) to take full advantage of the capabilities of the PC Interface. This terminal type is also non-initializing with no support of MIMs.

- Do not use telephones with data modules with the PC Interface. (You can still use 3270 Data Modules if you also use 3270 emulation). If you attach a DCP data module or ISDN data module to a telephone that is connected to a PC Interface card, the data module is bypassed (not used). All the interface functions are performed by the interface card even if a data module is present.
- The 7404D telephone with messaging cartridge cannot be used with PC Interface. However, the 7404D with PC cartridge can be used, but only with Group 1 configurations.

Wideband Switching

Wideband Switching provides the ability to dedicate 2 or more ISDN-PRI B-channels or DS0 endpoints for applications that require large bandwidth. It provides high-speed end-to-end communication between endpoints where dedicated facilities are not economic or appropriate. ISDN-BRI trunks do not support wideband switching.

Wideband Switching supports:

- High-speed video conferencing
- WAN disaster recovery
- Scheduled batch processing (for example, nightly file transfers)
- LAN interconnections and imaging
- Other applications involving high-speed data transmission, video transmission, or high bandwidth

Detailed description of Wideband Switching

ISDN-PRI divides a T1 or E1 trunk into 24 (32 for E1) channels, where one channel is used for signaling, and all others for standard narrowband communication. Certain applications, like video conferencing, require greater bandwidth. You can combine several narrowband channels into one wideband channel to accommodate the extra bandwidth requirement. Communication Manager serves as a gateway to many types of high-bandwidth traffic. In addition, DS1 Converter circuit packs are used for wideband switching at DS1 remote EPN locations. They are compatible with both a 24-channel T1 and 32-channel E1 facility (transmission equipment). They support circuit-switched wideband connections (NxDS0) and a 192 Kbps packet channel.

Wideband Switching channel type descriptions

The following table provides information on Wideband Switching channel types.

Channel Type	Number of Channels (DSOs)	Data Rate
H0 (T1 or E1)	6 (grouped 4 (T1) or 5 (E1) quadrants of 6 B-channels each)	384 Kbps
H11 (T1 or E1)	24 (on T1 - all 24 B-channels, with the D-channel not used; on E1 - B-channels 1 to 15, and 17 to 25, and B-channels 26 to 31 unused)	1536 Kbps
H12 (E1 only)	30 (B-channels 1 to 15 and 17 to 31)	1920 Kbps
NxDS0 (T1)	2-24	128 to 1536 Kbps
NxDS0 (E1)	2-31	128 to 1984 Kbps

Wideband switching channel allocation

For standard narrowband communication, ISDN-PRI divides a T1 or E1 trunk as follows:

- T1 trunks are divided into 23 information channels are 1 signaling channel
- E1 trunks are divided into 30 information channels, 1 signaling channel, and 1 framing channel

Certain applications, like video conferencing, require greater bandwidth. You can combine several narrowband channels into one wideband channel to accommodate the extra bandwidth requirement. Communication Manager serves as a gateway to many types of high-bandwidth traffic. In addition, DS1 converters are used for wideband switching at remote locations.

Performed using one of the three allocation algorithms: fixed, flexible, or floating.

- Fixed allocation — Provides contiguous-channel aggregation. The starting channel is constrained to a predetermined starting point. (Used only for H0, H11, and H12 calls.)
- Flexible allocation — Allows a wideband call to occupy non-contiguous positions within a single T1 or E1 facility (NxDS0).
- Floating allocation — Enforces contiguous-channel aggregation. The starting channel is not constrained to a predetermined starting point (NxDS0).

Wideband Switching video application example

A typical video application uses an ISDN-PRI interface to DS0 1 through 6 of the line-side facility. The figure on page 536 shows an example.

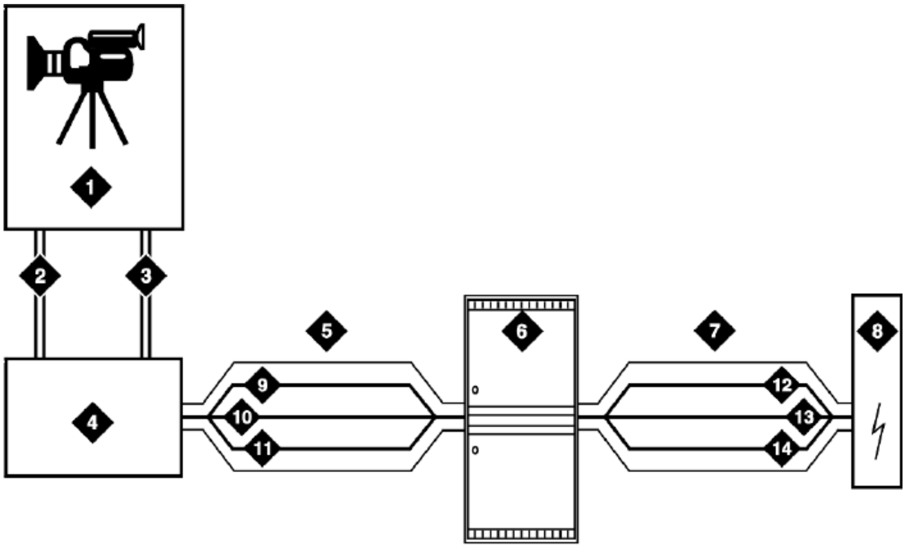


Figure 13: Typical video broadband application

Table 8: Figure notes:

1. Video application
2. Port 1
3. Port 2
4. ISDN terminal adaptor
5. Line-side ISDN-PRI
6. Avaya S8XXX Server
7. ISDN or ATM-CES trunk

1. Network
2. DS0 24 D-channel
3. DS0 23 unused
4. DS0 1-6 wideband
5. DS0 24 D-channel
6. DS0 7-23 narrow bands
7. DS0 1-6 wideband

ISDN-PRI terminal adapters with Wideband Switching

For Wideband Switching with non-ISDN-PRI equipment, you can use an ISDN-PRI terminal adapter. ISDN-PRI terminal adapters translate standard ISDN signaling into a form that can be used by the endpoint application, and vice versa. The terminal adapter also must adhere to the PRI-endpoint boundaries as administered on Communication Manager when handling both incoming applications to the endpoint and outgoing calls.

The terminal adapter passes calls to and receives calls from the line-side ISDN-SETUP messages. These messages indicate the data rate and the specific B-channels (DS0) to be used. The terminal adapter communicates all other call status information by way of standard ISDN messages. For more information, see *DEFINITY Line-Side ISDN Primary Rate Interface Technical Reference*.

Line-side T1 or E1 ISDN-PRI facilities with Wideband Switching

A line-side T1 or E1 ISDN-PRI facility is comprised of a group of DS0s. In this context, these DS0s are also called channels. T1 facilities have 23 B-channels and a single D-channel. E1 facilities have 30 B-channels, 1 D-channel, and a framing channel. Data flows bidirectionally across the facility between the server that is running Communication Manager and the ISDN-PRI terminal adapter.

PRI endpoints with Wideband Switching

A PRI-endpoint (PE) is a combination of DS0 B-channels on a line-side ISDN-PRI facility to which an extension is assigned.

A PE can support calls of lower bandwidth. In other words, a PE that has a width of six DS0 channels can handle a call of one channel of 64 Kbps, up to and including six channels totaling 384 Kbps. Also, a PE can support calls on nonadjacent channels. For example, an endpoint application that is connected to a PE that is defined as using B-channels 1 through 6 of an ISDN-PRI facility could use B-channels 1, 3, and 5 successfully to originate a call.

If the PE is administered to use flexible channel allocation, the algorithm for offering a call to the PE starts from the first DS0 that is administered to the PE. Since only one active call is permitted on a PE, contiguous B-channels are always selected unless one or more B-channels are not in service.

A PE remains in service unless all the B-channels are out of service. In other words, if B-channel 1 is out of service and the PE is five B-channels wide, the PE can still handle a wideband call of up to four B-channels wide. A PE can only be active on a single call at any given time. That is, the PE is considered to be idle, active or busy, or out of service.

One facility can support multiple separate and distinct PEs within a single facility. Non-overlapping contiguous sets of B-channel DS0s are associated with each PE.

Universal digital signal level 1 board

The universal digital signal level 1 (UDS1) board is the interface for line-side and network facilities that carries wideband calls.

Wideband Switching nonsignaling endpoint applications

Wideband Switching can also support configurations that use nonsignaling, non-ISDN-PRI line-side T1 or E1 facilities. The endpoint applications are the same as those that are defined for configurations with signaling.

Data service unit/channel service unit with Wideband Switching

The device service unit (DSU)/channel service unit (CSU) passes the call to the endpoint application. Unlike terminal adapters, the DSU/CSU does not have signaling capability.

Note:

No DSU/CSU is needed if the endpoint application has a fractional T1 interface.

Line-side (T1 or E1) facility with Wideband Switching

This facility, like the ISDN-PRI facility, is composed of a group of DS0s (24 for a T1 facility and 32 for an E1 facility; both T1 and E1 use 2 channels for signaling purposes). Line-side facilities are controlled solely from the server or Avaya S8XXX Server. Through the **`access-endpoint`** command, a specific DS0 or group of DS0s is assigned an extension. This individual DS0 or group, along with the extension, is known as a Wideband Access Endpoint (WAE).

Wideband access endpoint

WAEs have no signaling interface to the server or Avaya S8XXX Server. These endpoints simply transmit and receive wideband data when the connection is active.

Note:

Communication Manager can determine if the connection is active, but this does not necessarily mean that data is actually coming across the connection.

A WAE is treated as a single endpoint and can support only one call. If all DS0s comprising a wideband access endpoint are in service, then the wideband access endpoint is considered in service. Otherwise, the wideband access endpoint is considered out of service. If an in-service wideband access endpoint has no active calls on its DS0s, it is considered idle. Otherwise, the wideband access endpoint is considered busy.

Multiple WAEs are separate and distinct within the facility and endpoint applications must be administered to send and receive the correct data rate over the correct DS0s. An incoming call at the incorrect data rate is blocked.

Wideband Switching guidelines and examples

This section examines wideband and its components in relation to the following specific customer usage scenarios:

- Data backup connection
- Scheduled batch processing
- Primary data connectivity
- Networking

Wideband Switching data backup connection

Using Wideband Switching for data transmission backup provides customers with alternate transmission paths for critical data in the event of primary transmission path failure.

Wideband Switching scheduled batch processing

Scheduled batch processing applications are used for periodic database updates, such as retail inventory, or distributions, such as airline fare schedules. These updates are primarily done after business hours and are often referred to as “nightly file transfers”. Wideband meets the high bandwidth requirements at low cost for scheduled batch processing. Wideband also allows the dedicated-access bandwidth for busy-hour switching traffic to be used for these applications after business hours. Thus, no additional bandwidth costs are incurred.

The non-ISDN backup data connection is also appropriate for scheduled batch processing applications. Administered Connections are used to schedule daily or weekly sessions that originate from this application.

Wideband Switching primary data connectivity

Permanent data connections are well suited for Communication Manager when ISDN-PRI endpoints are used. Permanent data connections, such as interconnections between local area networks (LANs), are always active during business hours. The ISDN end-to-end monitoring and the ability of the endpoint to react to failures provide for critical availability of data. With ISDN, endpoints can detect network failures and initiate backup connections through the server. ISDN endpoints can also establish additional calls when extra bandwidth is needed.

Any failures that Communication Manager does not automatically restore are signaled to the endpoint application. The endpoint application can initiate backup data connections over the same PRI endpoint. Communication Manager routes the backup data connections over alternate facilities if necessary.

Wideband Switching networking

All wideband networking is over ISDN-PRI facilities, and the emulation of ISDN-PRI facilities by ATM-CES. Wideband networking may also connect to a variety of networks, other services of domestic interexchange carriers, private line, RBOC services, and services in other countries.

Wideband Switching ISDN-PRI trunk groups and channel allocation

Only ISDN-PRI trunks, and the emulation of ISDN-PRI trunks by ATM-CES, support wideband calls to the network. The bandwidth requirements of wideband calls necessitate modification of the algorithms by which trunks look for clear channels.

The following sections describe the search methods, and the relationship of those methods to the available wideband data services.

Facility lists and Wideband Switching

The system always sends a wideband call over a single trunk group and a single DS1 facility (or other ISDN-PRI-capable facility). Since a trunk group can contain channels (trunk members) from several different DS1 facilities, the system maintains a facility list for each trunk group.

A facility list orders the trunk members based on signaling group. If the system is using non-facility associated signaling groups with multiple DS1 facilities, the system sorts trunk members in that signaling group according to the interface identifier assigned to the corresponding DS1 facility.

When searching for available channels for a wideband call placed over a given trunk group, the system starts with the channels in the lowest-numbered signaling group with the lowest interface identifier. If the system cannot find enough channels in a given signaling group with that interface identifier, it checks the next higher interface identifier. If no more interface identifiers are available in the current signaling group, the system moves its search to the channels in the next higher signaling group.

For example, if three facilities having signaling group/interface identifier combinations of 1/1, 1/2, and 2/1 were associated with a trunk group, then a call offered to that trunk group would search those facilities in the order as they were just listed. Also note that since trunks within a given facility can span several trunk groups, a single facility can be associated with several different trunk groups.

Given this facility list concept, the algorithms have the ability to search for trunks, by facility, in an attempt to satisfy the bandwidth requirements of a given wideband call. If one facility does not have enough available bandwidth to support a given call, or it is not used for a given call due to the constraints presented in the following section, then the algorithm searches the next facility in the trunk group for the required bandwidth (if there is more than one facility in the trunk group).

In addition to searching for channels based on facilities and required bandwidth, Port Network (PN) preferential trunk routing is also employed. This PN routing applies within each algorithm at a higher priority than the constraints put on the algorithm by the parameters listed later in this section. In short, all facilities that reside on the same PN as the originating endpoint are searched in an attempt to satisfy the bandwidth of a given call, prior to searching any facilities on another PN.

Direction of trunk/hunting within facilities

You can tell the system to search for available channels in either ascending or descending order. These options help you reduce glare on the channels because the system can search for channels in the opposite direction to that used by the network. If an ISDN trunk group is not optioned for wideband, then a cyclical trunk hunt based on the administration of trunks within the trunk group is still available.

H11 channels

When a trunk group is administered to support H11, the algorithm to satisfy a call requiring 1,536 Kbps of bandwidth uses a fixed allocation scheme. That is, the algorithm searches for an available facility using the following facility-specific channel definitions:

- T1: H11 can only be carried on a facility without a D-channel being signaled in an NFAS arrangement (B-channels 1-24 are used).
- E1: Although the 1,536 Kbps bandwidth could be satisfied using a number of fixed starting points (for example, 1, 2, 3, and so forth), the only fixed starting point being supported is 1. Hence, B-channels 1-15 and 177-25 always are used to carry an H11 call on an E1 facility.

If the algorithm cannot find an available facility within the trunk that meets these constraints, then the call is blocked from using this trunk group. In this case, the call can be routed to a different trunk group preference via Generalized Route Selection (GRS), at which time, based on the wideband options administered on that trunk group, the call would be subject to another hunt algorithm (that is, either the same H11 algorithm or perhaps an N x DS0 algorithm described in a later paragraph).

Note that on a T1 facility, a D-channel is not considered a busy trunk and results in a facility with a D-channel always being partially contaminated. On an E1 facility, however, a D-channel is not considered a busy trunk because H11 and H12 calls can still be placed on that facility; an E1 facility with a D-channel and idle B-channels is considered an idle facility.

H12 channels

Since H12 is 1,920 Kbps, which is comprised of 30 B-channels, a 1,920-Kbps call can be carried only on an E1 facility. As with H11, the hunt algorithm uses a fixed allocation scheme with channel 1 being the fixed starting point. Hence, an H12 call is always carried on B-channels 1 through 15 and 17 through 31 on an E1 facility, as the following table shows. When the system is offered any other call other than a 1,536-Kbps call, the algorithm behaves as it does when H11 is optioned.

		DS0s that comprise each channel	
Facility	**ISDN interface**	**H11**	**H12**
T1	23B + D	-	-
T1	24B (NFAS)	1-24	-
E1	30B + D	1 through 15, 17 through 25	1 through 15, 17 through 31
E1	31B (NFAS)	1 through 15, 17 through 25	1 through 15, 17 through 31

H0 channels

When a trunk group is administered to support H0, the algorithm to satisfy a call requiring 384 Kbps of bandwidth also uses a fixed allocation scheme. Unlike the H11 fixed scheme which only supports a single fixed starting point, the H0 fixed scheme supports 4 (T1) or 5 (E1) starting points. The H0 algorithm searches for an available quadrant within a facility based on the direction of trunk or hunt administered. If the algorithm cannot find an available quadrant within any facility allocated to this trunk group, then the call is blocked from using this trunk group. Again, based on GRS administration, the call might route to a different trunk group preference and be subject to another algorithm based on the wideband options administered.

Note that a D-channel is considered a busy trunk and results in the top most quadrant of a T1, B-channels 19 to 24, always being partially contaminated. This is *not true* for NFAS.

If this H0 optioned trunk group is also administered to support H11, H12, or N x DS0, then the system also attempts to preserve idle facilities. In other words, when offered a narrowband, H0, or N x DS0 call, the system searches partially-contaminated facilities before it searches to idle facilities.

N x DS0 channels

For the N x DS0 multi-rate service, a trunk group parameter determines whether a floating or a flexible trunk allocation scheme is to be used. The algorithm to satisfy an N x DS0 call is either floating or flexible.

- Floating (Contiguous) — In the floating scheme, an N x DS0 call is placed on a contiguous group of B-channels large enough to satisfy the requested bandwidth without any constraint being put on the starting channel (that is, no fixed starting point trunk).
- Flexible — In the flexible scheme, an N x DS0 call is placed on any set of B-channels as long as the requested bandwidth is satisfied. There is absolutely no constraint such as contiguity of B-channels or fixed starting points. Of course, as with all wideband calls, all the B-channels comprising the wideband call must reside on the same ISDN facility.

  Regardless of the allocation scheme employed, the N x DS0 algorithm, like the H11 and H12 algorithms, attempts to preserve idle facilities when offered B, H0, and N x DS0 calls. This is important so that N x DS0 calls, for large values of N, have a better chance of being satisfied by a given trunk group. However, if one of these calls cannot be satisfied by a partially-contaminated facility and an idle facility exists, a trunk on that idle facility is selected, thus contaminating that facility.

  There are additional factors to note regarding specific values of N and the N x DS0 service:

  - N = 1 — this is considered a narrowband call and is treated as any other voice or narrowband-data (B-channel) call.
  - N = 6 — if a trunk group is optioned for both H0 and N x DS0 service, a 384-kbps call offered to that trunk group is treated as an H0 call and the H0 constraints apply. If the H0 constraints cannot be met, then the call is blocked.
  - N = 24 — if a trunk group is optioned for both H11 and N x DS0 service, a 1,536-kbps call offered to that trunk group is treated as an H11 call and the H11 trunk allocation constraints apply.

- N = 30 — if a trunk group is optioned for both H12 and N x DS0 service, a 1,920-kbps call offered to that trunk group is treated as an H12 call and the H12 trunk allocation constraints apply.

Wideband Switching glare and blocking prevention

Wideband Switching glare prevention

Glare occurs when both sides of an ISDN interface select the same B-channel for call initiation. For example, a user side of an interface selects the B-channel for an outgoing call and, before Communication Manager receives and processes the SETUP message, the server also selects the same B-channel for call origination. Since any single wideband call uses more channels, the chances of glare are greater. With proper and careful administration, glare conditions can be reduced.

To reduce glare probability, the network needs to be administered so both sides of the interface select channels from opposite ends of facilities. This is called linear hunting, ascending or descending. For example, on a 23B+D trunk group, the user side could be administered to select B-channels starting at channel 23 while the network side would be administered to start selecting at channel 1. Using the same example, if channel 22 is active but channel 23 is idle, the user side should select channel 23 for re-use.

Wideband Switching blocking prevention

Blocking occurs when an insufficient number of B-channels are available to make a call. Narrowband calls require only one channel, so blocking is less likely than with wideband calls that require multiple B-channels. Blocking also occurs for wideband calls when bandwidth is not available in the appropriate format, such as fixed, floating, or flexible.

To reduce blocking, Communication Manager selects trunks for both wideband calls and narrowband calls to maximize the availability of idle fixed channels for H0, H11, and H12 calls, and idle floating channels for N x DS0 calls that require a contiguous bandwidth. The strategy for preserving idle channels depends on the channel type. The chances for blocking are reduced if you use a flexible algorithm, assuming that the algorithm is supported on the other end.

The following table describes the blocking strategy for the different channel types.

Channel type	Blocking minimization strategy
H0	Preserve idle quadrants
H11	Preserve idle facilities
H12	Preserve idle facilities

Channel type	Blocking minimization strategy
Flexible N x DS0	Preserve idle facilities
Floating N x DS0	Preserve idle facilities as first priority

Administering Wideband Switching

About this task

Before you start, you need a DS1 Converter circuit pack.

Procedure

1. On the Access Endpoint screen, administer all fields.
2. On the PRI Endpoint screen, administer all fields.
3. On the ISDN Trunk Group screen, administer all fields.
4. On the Route Pattern screen, administer all fields.

Considerations for Wideband Switching

- For wideband switching with non-ISDN-PRI equipment, you can use an ISDN-PRI terminal adapter.

Interactions for Wideband Switching

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

Administered Connections

Administered Connections provides call initiation for wideband access endpoints (WAEs). All Administered Connections that originate from WAEs use the entire bandwidth that is administered for WAE. The destination of an Administered Connection can be a PRI endpoint.

Automatic Circuit Assurance (ACA)

ACA treats wideband calls as single-trunk calls so that a single ACA-referral call is made if an ACA-referral call is required. The call is on the lowest B-channel that is associated with the wideband call.

Call Coverage

A WAE cannot be administered as a coverage point in a call-coverage path.

Call Detail Recording (CDR)

When CDR is active for the trunk group, all wideband calls generate CDR records. The CDR feature flag indicates a data call, and CDR records contain bandwidth and Bearer Capability Class (BCC).

Call Forwarding

You must block Call Forwarding through Class of Service (COS).

Call Management System (CMS) and Basic Call Management System (BCMS)

Wideband calls can be carried over trunks that are measured by CMS and BCMS. Wideband endpoints are not measured by CMS and BCMS.

Call Vectoring

PRI endpoints use a vector directory number (VDN) to dial. For example, PRI endpoint 1001 dials VDN 500. VDN 500 points to Vector 1. Vector 1 can point to other PRI endpoints such as route-to 1002, or route-to 1003, or busy.

Certain applications use Call Vectoring. When an incoming wideband call hunts for an available wideband endpoint, the call can point to a VDN, that sends the call to the first available PRI endpoint.

Class of Restriction (COR)

COR identifies caller and called-party privileges for PRI endpoints. Administer the COR so that account codes are not required. Forced entry of account codes (FEAC) is turned off for wideband endpoints.

Class of Service (COS)

COS determines the class of features that a wideband endpoint can activate.

Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS)

FAS and NFAS with or without D-Channel Backup requires administration by way of signaling groups for trunk-side wideband interfaces.

Facility Busy Indication

You can administer a busy-indicator button for a wideband-endpoint extension, but the button does not accurately track endpoint status.

Facility Test Calls

Use Facility Test Calls to perform loop-back testing of the wideband call facility.

Generalized Route Selection (GRS)

GRS supports wideband BCC to identify wideband calls. GRS searches a route pattern for a preference that has wideband BCC. Route preferences that support wideband BCC also support other BCCs to allow different call types to share the same trunk group.

CO Trunk (TTC - Japan) Circuit Pack

The CO Trunk (TTC - Japan) circuit pack cannot perform wideband switching. No member of the circuit pack should be a member of a wideband group.

CallVisor Adjunct-Switch Applications Interface

CallVisor Adjunct-Switch Applications Interface (ASAI) links Communication Manager and adjunct applications. The interface allows adjunct applications to access switching features and supply routing information to Communication Manager. CallVisor ASAI improves Automatic Call Distribution (ACD) agents' call handling efficiency by allowing an adjunct to monitor, initiate, control, and terminate calls on the Avaya S8XXX Server. The CallVisor ASAI interface can be used for Inbound Call Management (ICM), Outbound Call Management (OCM), and office automation/messaging applications.

CallVisor ASAI is supported by two transport types. These are:

1. Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) transport (CallVisor ASAI-BRI)
2. LAN Gateway Transmission Control Protocol/Internet Protocol transport (Avaya LAN Gateway).

CallVisor ASAI messages and procedures are based on the ITU-T Q.932 international standard for supplementary services. The Q.932 Facility Information Element (FIE) carries the CallVisor ASAI requests and responses across the interface. An application program can access CallVisor ASAI services by supporting the ASAI protocol or by using a third-party vendor application programming interface (API).

ASAI configuration example

For a simple ASAI configuration example, see the figure on page 546.

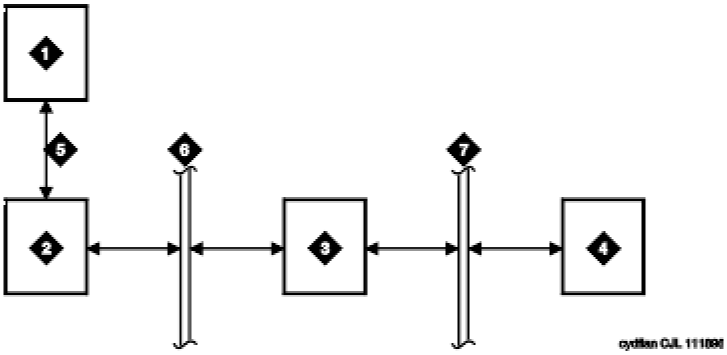


Figure 14: ASAI Switch Interface Link — BRI Transport

Table 9: Figure notes:

1. ASAI adjunct	1. ISDN-BRI
2. ISDN Line circuit pack	2. Packet bus
3. Packet Controller circuit pack	3. Memory bus
4. Switch processing element (SPE)	

ASAI Capabilities

For information concerning the types of associations over which various event reports can be sent, see *Communication Manager ASAI Technical Reference*, 555-230-220.

Considerations for ASAI

- If your system has an expansion cabinet (with or without duplication), ASAI resources should reside on the system's Processor Cabinet.

Interactions for ASAI

See *Communication Manager ASAI Technical Reference*, 555-230-220.

CallVisor ASAI setup

CallVisor Adjunct-Switch Applications Interface (ASAI) can be used in the telemarketing and help-desk environments. It is used to allow adjunct applications to monitor and control resources in Communication Manager.

Preparing to set up ASAI

Procedure

On the System Parameters Customer-Options (Optional Features) screen, verify that the:

- **ASAI Link Core Capabilities** field is `y`. If not, contact your Avaya representative.

- **Computer Telephony Adjunct Links** field is `y` if the adjunct is running the CentreVu Computer Telephony.

Setting up ASAI

About this task

To set up CallVisor ASAI:

Procedure

1. Type `add cti-link` *nn*, where *nn* is a number between 1 and 64.

   Press `Enter`.

   The system displays the CTI Link screen.
2. In the **Type** field, type
   - `asai` if this adjunct platform is other than CentreVu Computer Telephony, for example, IBM CallPath.
   - `adjlk` (Computer Telephony adjunct link) if this is for the CentreVu Computer Telephony using the Telephony Services Application Programming Interface (TSAPI).
3. In the **Port** field, use the port address assigned to the LAN Gateway Interface circuit pack.
4. Press **Enter** to save your changes.

Chapter 19: Collecting Call Information

Call information collection

Call Detail Recording (CDR) collects detailed information about all incoming and outgoing calls on specified trunk groups. If you use Intra-switch CDR, you can also collect information about calls between designated extensions on Communication Manager. Communication Manager sends this information to a printer or to some other CDR output device that collects call records and that might also provide reports.

You can have a call accounting system directly connected to your Avaya S8XXX Server running Communication Manager. If you are recording call details from several servers, Communication Manager can send the records to a collection device for storage. A system called a poller can then take these records and send them to the call accounting system. The call accounting system sorts them, and produces reports that you can use to compute call costs, allocate charges, analyze calling patterns, detect unauthorized calls, and keep track of unnecessary calls.

Requirements for administering call accounting

The call accounting system that you use might be sold by Avaya, or it might come from a different vendor. You need to know how your call accounting system is set up, what type of call accounting system or call detail recording unit you are using, and how it is connected to the server running Communication Manager. You also need to know the format of record that your call accounting system requires.

⚠ **Caution:**

When migrating a platform from a legacy system to a Linux-based system of Communication Manager 3.0 or newer, where both the old and new systems utilize CDR, ensure that the older CDR parsing scripts correctly utilize all of the characters identified in each of the fields contained in the applicable format table (see the Format Tables in the *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205).

Setting up CDR example

About this task

In this example, we are going to establish call detail recording for all calls that come in on trunk group 1 (our CO trunk). We are going to set up CDR so that any call that is handled by an attendant produces a separate record for the attendant part of the call.

Procedure

1. Enter **`change trunk-group n`**.
2. In the **CDR Reports** field, enter `y`.

   This tells Communication Manager to create call records for calls made over this trunk group.
3. Select `Enter` to save your changes.
4. Enter `change system-parameters cdr`.
5. In the **CDR Format** field, type `month/day`.

   This determines how the date will appear on the header record.
6. In the **Primary Output Format** field, enter `Unformatted`.

   This is the record format that our call accounting system requires. Check with your call accounting vendor to determine the correct record format for your system.
7. In the **Use Legacy CDR Formats** field, enter `y` to use CDR formats from Communication Manager 3.1 and earlier.
8. Enter `n` to use formats from Communication Manager 4.0 and later.

   (For more information, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, **Use Legacy CDR Formats** field.)
9. In the **Primary Output Ext.** field, enter `2055`.

   This is the extension of the data module that we use to connect to our call accounting system.
10. In the **Record Outgoing Calls Only** field, enter `n`.

    This tells Communication Manager to create records for both incoming and outgoing calls over all trunk groups that use CDR.
11. In the **Outg Trk Call Splitting** and **Inc Trk Call Splitting** fields, enter `y`.

    This tells the system to create a separate record for any portion of an incoming or outgoing call that is transferred or conferenced.
12. In the **Outg Att Call Record** and **Inc Att Call Record** fields, enter `y`.

    This tells the system to create a separate record for the attendant portion of any incoming or outgoing call.

You can also administer Communication Manager to produce separate records for calls that are conferenced or transferred. This is called Call Splitting. There are many other variations that you can administer for CDR.

For additional information on Call Detail Recording (CDR), see *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Intra-switch CDR administration

Call detail recording generally records only those calls either originating or terminating outside the server running Communication Manager. There might be times when you need to record calls between users on the local server. Intra-switch CDR lets you track calls made to and from local extensions.

Setting up intra-switch CDR example

Procedure

1. In this example, we administer Communication Manager to record all calls to and from extensions 5100, 5101, and 5102.
2. Type **`change system-parameters cdr`** and select `Enter`.
3. In the **intra-switch CDR** field, enter `y` and select `Enter` to save your changes.
4. Type **`change intra-switch-cdr`** and select `Enter`.
5. In the first three available slots, enter `5100`, `5101`, and `5102`.
6. Select `Enter` to save your changes.

   Communication Manager will now produce call records for all calls to and from these extensions, including those that originated on the local server.

   See Intra-Switch CDR in *Avaya Aura™ Communication Manager* Screen Reference, 03-602878, for more detailed information.

Account Code call tracking

You can have your users to enter account codes before they make calls. By doing this, you can have a record of how much time was spent on the telephone doing business with or for a particular client.

Setting up Account Code call tracking example

About this task

In this example, we are going to set up the system to allow the user at extension 5004 to enter a 5-digit account code before making a call.

Procedure

1. Enter **`change system-parameters cdr`**.
2. In the **CDR Account Code Length** field, type `5` and select `Enter` to save your changes.
3. Assign an account button on the **Station** screen for extension 5004.
4. Provide your users with a list of account codes to use.
5. You can also assign a feature access code and give this to your users.

Forced Entry of Account Codes

Forced Entry of Account Codes is another form of account code dialing. You can use it to allow certain types of calls only with an account code, to track fax machine usage by account, or just to make sure that you get account information on all relevant calls.

Preparing to administer Forced Entry of Account Codes

Procedure

Verify that Forced Entry of Account Codes is enabled on the System Parameters Customer-Options (Optional Features) screens.

If it is not, contact your Avaya representative.

Administering Forced Entry of Account Codes example

About this task

In this example, we administer the system to force users in our North American office to enter an account code before making international calls.

Procedure

1. Type **`change system-parameters cdr`** and select `Enter`.
2. In the **Force Entry of Acct Code for Calls Marked on Toll Analysis Form** field, type `y`.
3. In the **CDR Account Code Length** field, type `5` and select `Enter` to save your changes.
4. Type **`change toll 0`**.

   Press `Enter`.
5. The system displays the Toll Analysis screen.
6. In the first available **Dialed String** field, type `011`.

   This is the international access code for this office.
7. In the **Total Min** and **Max** columns, type `10` and `18`, respectively.

   This is the minimum and maximum number of digits the system will analyze when determining how to handle the call.
8. In the **Toll List** and **CDR FEAC** columns, type `x`.
9. Press `Enter` to save your changes.

   You can also establish a class of restriction with **Forced Entry of Account Codes** set to `y`, and assign this class of restriction (COR) to trunks or other facilities that you want to restrict. With this method, all users with this COR must enter account codes before making any outgoing trunk calls. See Class of Restriction in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information.

Public network Call-Charge Information administration

Communication Manager provides two ways to receive information from the public network about the cost of calls. Note that this service is not offered by the public network in some countries, including the US.

- Advice of Charge (AOC, for ISDN trunks) collects charge information from the public network for each outgoing call. Charge advice is a number representing the cost of a call; it might be recorded as either a charging or currency unit.
- Periodic Pulse Metering (PPM, for non-ISDN trunks) accumulates pulses transmitted from the public network at periodic intervals during an outgoing trunk call. At the end of the call, the number of pulses collected is the basis for determining charges.

For more information about AOC and PPM, see Call Charge Information in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Preparing to administer public network call-charge information

Procedure

You need to request either AOC or PPM service from your network provider.

In some areas, your choice might be limited. Your Avaya technical support representative can help you determine the type of service you need.

Note:

This service is not offered by the public network in some countries, including the U.S.

Collecting call charge information over ISDN example

About this task

In this example, we administer the system to provide Advice of Charge over an existing ISDN trunk group, at the end of a call. This information will appear on CDR reports.

Procedure

1. Enter **`change trunk-group 2`**.
2. In the **CDR Reports** field, type `y`.

This ensures that the AOC information appears on the CDR report.

3. Verify that **Service Type** is `public-ntwrk`.
4. In the **Supplementary Service Protocol** field, enter `a`.
5. The **Charge Advice** field, enter `end-on-request`.

   This ensures that Communication Manager will place one request for charge information. This reduces the amount of information passed to Communication Manager and consumes less processor time than other options.
6. Select `Enter` to save your changes.

Charge Advice for QSIG trunks administration

Use the QSIG Supplementary Service - Advice of Charge feature to extend charging information from the public network into the private network. The charging information that many service providers supply is extended from a gateway enterprise system to the end user's enterprise system. The charging information can then be displayed on the user's desktop.

Information can be extended and displayed either:

- At intervals during the call and at the end of the call, or
- Only at the end of the call

QSIG stands for Q-Signaling, which is a common channel signal protocol based on ISDN Q.931 standards and used by many digital telecommunications systems. Only charge information received from the public network with ETSI Advice of Charge, and Japan Charge Advice is extended into the QSIG private network.

Administering Charge Advice for QSIG

Procedure

1. On the Trunk Group screen, for Group Type **ISDN**, <tab> to the **Charge Advice** field.
2. Select from the following options:
   - during-on-request - to request that charging information be provided at intervals during a call, and also at the end of the call
   - end-on request - to request that charging information be provided only at the end of a call
   - none - no charging information will be requested for the trunk group

Note:

Receipt of charge advice on the QSIG trunk group is also dependent on Charge Advice administration at the PSTN trunk group involved on the call, and whether charges are received from the public network.

3. On the **Trunk Group** screen, administer the **Decimal Point** field.

   - period (.) -This is the default. If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a period as the decimal point.
   - comma (,) - If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a comma as the decimal point.

   If the received charge contains no decimals, no decimal point is displayed (that is, the administered decimal point is ignored for charge information received with no decimals). On an upgrade from a QSIG trunk group with the **Decimal Point** field administered as `none`, the field defaults to **period**.

Receiving call-charge information over non-ISDN trunks example

About this task

In this example, we will administer an existing Direct Inward and Outward Dialing (DIOD) trunk to receive PPM from the public network.

Procedure

1. Type **`change trunk-group 3`**.

   The system displays the Trunk Group screen with existing administration for this trunk group. Click the numbered page tabs or **Next Page** to find fields that appear on subsequent pages of the Trunk Group screen.

2. In the **CDR Reports** field, type `y`.

   This ensures that the PPM information appears on the CDR report.

3. In the **Direction** field, enter `two-way`.

4. Click **Next Page** to find the **PPM** field.

5. In the **PPM** field, enter `y`.

6. In the **Frequency** field, enter `50/12`.

   This is the signal frequency (in kHz). The frequency you will use depends on what the circuit pack you use is able to accept. See Tone Generation in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information.

7. In the **Administrable Timers** section, set the **Outgoing Glare Guard** timer to `5` seconds and select **Enter** to save your changes.
8. You also need to ensure that the values of the **Digital Metering Pulse Minimum**, **Maximum** and **Value** on the DS1 Circuit Pack screen are appropriate to the values offered by your service provider.

Viewing Call Charge Information example

About this task

Communication Manager provides two ways for you to view call-charge information: on a telephone display or as part of the Call Detail Recording (CDR) report. From a display, users can see the cost of an outgoing call, both while the call is in progress and at the end of the call.

In this example, we administer extension 5040 to be able to view the charge of a call in progress. The charges will appear in currency units (in this case, Lira) on the user's telephone display.

Procedure

1. Enter `change trunk-group 2` .
2. Click **Next Page** until you see the **Trunk Features** section.
3. In the **Charge Conversion** field, enter `200`.

   This indicates that one charge unit sent from the service provider is equal to 200 units, in this case, Lira.
4. In the **Decimal Point** field, enter `none`.
5. In the **Charge Type** field, enter `Lira` and select `Enter` to save your changes.
6. Enter `change system-parameters features`.
7. In the Charge Display Update Frequency (seconds) field, enter `30` and select `Enter` to save your changes.

   Frequent display updates might have considerable performance impact.
8. Now assign extension 5040 a **disp-chrg** button to give this user the ability to control the charge display.

   See Adding Feature Buttons for more information.

   If you want end users to control when they view this information, you can assign a display button that they can press to see the current call charges. If you want call charges to display automatically whenever a user places an outgoing call, you can set **Automatic Charge Display** to `y` on the user's COR screen.

Survivable CDR detailed description

The Survivable CDR feature is used to store CDR records to a server's hard disk. For Survivable Core andSurvivable Remote Servers, the Survivable CDR feature is used to store the CDR records generated from calls that occur when a Survivable Remote or Survivable Core Server is controlling one or more gateways or port networks. For a main server, the Survivable CDR feature provides the ability to store CDR records on the server's hard disk.

When the Survivable CDR feature is enabled, the CDR records are saved in a special directory named `/var/home/ftp/CDR` on the server's hard disk. The CDR adjunct retrieves the Survivable CDR data files by logging into the server and copying the files to its own storage device. The CDR adjunct uses a special login that is restricted to only accessing the directory where the CDR records are stored. After all the files are successfully copied, the CDR adjunct deletes the files from the server's hard disk and processes the CDR records in the same manner that it does today.

Note:

This feature is available on main servers and Survivable Core Servers that are Communication Manager Release 5.0 and later releases only. It is available on Survivable Remote platforms running Communication Manager 4.0 and later.

The CDR adjunct must poll each main, Survivable Remote Server, and Survivable Core Server regularly to see if there are any new data files to be collected. This is required even when a Survivable Remote or Survivable Core Server is not controlling a gateway or a port network because the CDR adjunct has no way of knowing if a Survivable Remote or Survivable Core Server is active.

The Survivable CDR feature utilizes the same CDR data file formats that are available with legacy CDR.

Files for Survivable CDR

When Survivable CDR is enabled, the server writes the CDR data to files on the hard disk instead of sending the CDR data over an IP link. The Survivable CDR feature creates two types of CDR data files: a Current CDR data file that the server uses to actively write CDR data and a set of archive files containing CDR data that the server collected earlier but has not yet been collected and processed by the CDR adjunct. The naming convention for both file types are similar. However the name of the Current CDR file is always prefixed by a "C-" (for more information, see File naming conventions for Survivable CDR). The CDR Current file remains active until one of the following events happen:

- The server's system clock reaches 12:00 midnight.
- The Current CDR file reaches or exceeds 20 megabytes. A 20 megabyte file may contain up to 140K CDR records depending on the CDR format used.
- A filesync, a reset system 2 (cold restart), or a reset system 4 (reboot) occurs.

After one of the above events occur the following actions take place:

- The Current CDR file is closed and it becomes an archive CDR file.
- The file permissions change from `read/write (rw)` for root and read only for members of the CDR_User group to:
    - Owner (root): `Read/Write/Execute (rwx)`
    - Group (CDR_User): `Read/Write (rw-)`
    - World: `none (---)`
- The "C-" prefix is removed from the front of the file name
- For a main server, a new Current CDR file is created
- For a Survivable Remote or Survivable Core Server, a new Current CDR file is created only if the Survivable Remote or Survivable Core Server is controlling one or more gateways or port networks.

File naming conventions for Survivable CDR

The Survivable CDR data files have the following naming conventions:

```
tssssss-cccc-YYMMDD-hh_mm
```

where:

- `t` is populated with an L for a Survivable Remote Server, an E for a Survivable Core Server, or an S for a main server
- `ssssss` is populated with the least significant six digits of the System ID or SID. The SID is a unique number in the RFA license file used to identify the system. The SID for a server can be viewed by using one of the following methods:
    - Use the **`statuslicense -v`** BASH command.
    - Use the command **`display system-parameters customer-options`** on the SAT.
- `cccc` is populated with the least significant four digits of the Cluster ID (CL ID) or Module ID (MID). To display the MID for the server:

  - Use the **statuslicense -v** BASH command.

- YY is populated with the two digit number of the year the file was created.
- MM is populated with the two digit number of the month the file was created.
- DD is populated with the two digit day of the month the file was created.
- hh is populated with the hour of the day the file was created based on a 24 hour clock.
- mm is populated with the number of minutes after the hour when the file was created.

The Current CDR file uses the same naming convention except the name is prefixed with a "C-".

Survivable CDR file removal

You can remove CDR files by:

The Survivable CDR feature

The Survivable CDR feature on the main, Survivable Remote Server, or Survivable Core Server automatically removes the oldest CDR data achieve file anytime the number of archived files exceed 20. The Current CDR file is not an archived file and therefore not counted in the 20 files allowed on the hard disk.

CDR adjunct

In a normal operating environment, the CDR adjunct has the responsibility to delete the CDR data files after they are copied and verified that they are correct.

Survivable CDR file access

A special user group called CDR_User exists that allows the administrator to identify all users authorized to access the CDR storage directory. The archived CDR files are stored in`/var/home/ftp/CDR`.

Administering Survivable CDR

Procedure

1. Create a new user account to allow the CDR adjunct access and permissions to retrieve CDR data files, see Creating a new user account.

2. Enable CDR storage on the hard disk, see Administering Survivable CDR for the main server.
3. If using this feature on the main server: Administer the **Primary Output Endpoint** field on the main's `change system-parameters cdr` SAT form to be DISK, see Administering Survivable CDR for the main server.

   When using Survivable CDR, only the **Primary Output Endpoint** field is available. Administration of the **Secondary Output Endpoint** field is blocked.
4. If you are using this feature on a Survivable Remote Server and a Survivable Core Server: Administer the **Enable CDR Storage on Disk** field on the change survivable-processor screen, see Administering Survivable CDR for a Survivable Remote or Survivable Core Server.

Creating a new CDR user account

About this task

For the CDR adjunct to access the CDR data files, a new user account must be created on the main server. The new account is pushed to the Survivable Remote and/or Survivable Core Server when a filesync is performed.

Procedure

1. On the Server Administration Interface, click **Administrator Accounts** under the Security heading.
2. On the Administrator Accounts page, enter the login ID for the new user in the **Enter Login ID or Group Name** field.
3. Click the **Add Login** radio button and then click **Submit**.
4. On the Administrator Logins -- Add Login page, enter the data in the table on page 561 in each field.

   Table 10: CDR adjunct user account recommended options

Field Name	Recommended Option
Login Name	Any valid user name chosen by the administrator or installer
Login group	CDR_User
Shell:	Select CDR access only by clicking the associated radio button.
Lock this account	Leave blank

Field Name	Recommended Option
Date on which the account is disabled	Leave blank
Select type of authentication	Password
Enter key or password	Any valid password chosen by the administrator or installer
Re-enter key or password	Re-enter the above password
Force password/key change on first login	no
Maximum Number of days a password may be used (PASS_MAX_DAYS)	99999
Minimum number of days allowed between password changes (PASS_MIN_DAYS)	0
Number of days warning given before a password expires (PASS_WARN_AGE)	7
Days after password expires to lock account	-1

5. Click **Add** to create the new user account.

Administering Survivable CDR for the main server

Procedure

On the **system-parameters cdr** screen:

a. **Enable CDR Storage on Disk?**: Possible entries for this field are yes or no.

Entering yes in this field enables the Survivable CDR feature for the main, Survivable Remote Server, and Survivable Core Server. If this field is set to no, the CDR functionality remains as legacy CDR.

b. **Primary Output Endpoint**: Possible entries for this field are CDR1, CDR2, and DISK.

For the main server, the **Primary Output Endpoint** field must be set to DISK. When Survivable CDR is administered as Disk on the **Primary Output Endpoint** field, the **Secondary Output Endpoint** field is blocked.

Administering Survivable CDR for a Survivable Remote or Survivable Core Server

About this task

Note:

The Survivable CDR feature is administered on the main server for the Survivable Remote and Survivable Core Servers.

Important:

A Survivable Remote or Survivable Core Server only stores Survivable CDR records if it is administered to support Survivable CDR and if it is controlling one or more gateways or port networks.

Procedure

1. On the **system-parameters cdr** screen:

   Enable CDR Storage on Disk: Possible entries for this field are yes or no.

   Entering yes in this field enables the Survivable CDR feature for the main, Survivable Remote, and Survivable Core Servers. If this field is set to no, the CDR functionality remains legacy CDR.

2. On the Survivable-processor screen:

   a. **Service Type**: The **Service Type** field must be set to CDR1 or CDR2 to enable entries to the **Store to Dsk** field.

   b. **Store to Dsk**: Enter `y` to enable Survivable CDR for this Survivable Remote or Survivable Core Server.

      When the **Service Type** field is set to CDR1 or CDR2 and the **Store to Dsk** field is set to yes, all CDR data for the specific Survivable Remote or Survivable Core Server being administered will be sent to the hard disk rather than output to an IP link. Survivable Remote or Survivable Core Server will only store CDR records to hard disk when the Survivable Remote or Survivable Core Server is controlling a gateway or port network.

   Important:

   You must complete the Survivable Processor screen for each Survivable Remote or Survivable Core Server that will utilize the Survivable CDR feature.

Note:

The **Enable** field for a given line in the change survivable-processor screen must be set to “o” (overwrite) to allow changes for that line.

Communication Manager SIP Video Infrastructure Enhancements

Note:

Communication Manager 6.0 as a SIP feature server implies that Communication Manager is configured with IMS enabled SIP signaling interfaces that are connected to the Session Manager 6.0. The H.323 calls are not routed via the feature server and therefore, only SIP requirements impact feature server operation. From Release 6.0 Communication Manager is supported as an Access Element as well.

- Communication Manager 6.0 supports SIP video and audio shuffling optimization.
- Communication Manager reduces the total memory footprint of each SIP call leg that has video enabled by no longer storing a duplicate copy of far-end caps in the SIP user manager.
- Communication Manager does not allocate video structures internally when only audio media is present in the SDP for the initial dialog.
- Communication Manager indicates when the called party is a video enabled endpoint and hence allows video to be added when a called party is transferred or conferenced via sending a re-INVITE (no SDP) to trigger renegotiation of capabilities by both endpoints in the new call topology.
- Communication Manager has its capacity for SIP video calls set to 1/3 of the capacity for all SIP calls. This is the equivalent ratio of audio/video users with the current H.323 solution. This change ensures that SIP video capacity increases along with SIP audio capacity in a defined manner and as the work to increase audio calls is completed, additional video calls are supported.
- Communication Manager initiates video OLCs to H.323 MCUs on behalf of SIP endpoints.
- All existing Communication Manager H.323 functionality and compatibility with both Polycom and Meeting Exchange must be maintained. Versions of Polycom firmware as tested for CM 5.2 need to be verified against the Communication Manager 6.0 . The existing H.323 functionality also need to be verified against new One X Communicator 6.0 and Meeting Exchange firmwares.
- Communication Manager as a feature server supports negotiation between endpoints of a video fast-update mechanism using RTCP feedback as specified in RFC4585 and RFC5104.

- Communication Manager as a feature server supports negotiation between endpoints of a video flow-control (Temporary Maximum Media Bitrate Request) mechanism using RTCP feedback as specified in RFC4585 and RFC5104.
- Communication Manager implements simplified SIP call flows by removing the need to “black hole” video media in the initial SIP INVITE when direct media is enabled.
- Communication Manager as a feature server passes through any media sessions which it does not explicitly handle to tandem dialogs.

Chapter 20: Managing System Platform virtual machines

Virtual Machine Management

Use the options under Virtual Machine Management to view details and manage the virtual machines on System Platform. Some of the management activities that you can perform include rebooting or shutting down a virtual machine.

The System Domain (Dom-0), Console Domain, and components of the solution templates running on the System Platform are known as virtual machines. The System Domain (Dom-0) runs the virtualization engine and has no direct management access. Console Domain (cdom or udom) provides management access to the system through the System Platform Web Console.

Solution template

After installing System Platform, you can install various solutions templates to run on System Platform. After installing the templates, you can manage the templates from the System Platform Web Console.

Viewing virtual machines

Procedure

1. Click **Home** or click **Virtual Machine Management** > **Manage**.
   The Virtual Machine List page displays a list of all the virtual machines that are currently running on the system.
2. To view details of a specific virtual machine, click the virtual machine name.

The Virtual Machine Configuration Parameters page displays configuration details for the virtual machine, including its MAC address, IP address, and operating system.

Related topics:
[Virtual Machine List field descriptions](#) on page 569
[Virtual Machine Configuration Parameters field descriptions](#) on page 571

Rebooting a virtual machine

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. On the Virtual Machine List page, click the virtual machine name which you want to reboot.
3. On the Virtual Machine Configuration Parameters page, click **Reboot**.

Related topics:
[Virtual Machine List field descriptions](#) on page 569
[Virtual Machine Configuration Parameters field descriptions](#) on page 571

Shutting down a virtual machine

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. If you want to stop a virtual machine, then click the entry corresponding to the virtual machine name on the Virtual Machine List page.
   On the Virtual Machine Configuration Parameters page, click **Stop**.

   > **Note:**
   >
   > The Console Domain can only be restarted and not stopped. If the Console Domain is stopped, administration of the system will no longer be possible.

3. If you want to shutdown the entire server including all of the virtual machines, perform one of the following steps:

- On the Virtual Machine List page, click **Domain-0** in the **Name** column.

  On the Virtual Machine Configuration Parameters page, click **Shutdown Server**.
- Click **Server Management** > **Server Reboot / Shutdown**.

  On the Server Reboot/Shutdown page, click **Shutdown Server**.

Related topics:

Virtual Machine List field descriptions on page 569

Virtual Machine Configuration Parameters field descriptions on page 571

Virtual Machine List field descriptions

The Virtual Machine List page displays a list of all the virtual machines currently running in the system.

Name	Description
Name	Name of the virtual machines running on System Platform.
Version	Version number of the respective virtual machine.
IP Address	IP address of the virtual machine.
Maximum Memory	This is a display only field. The value is set by Avaya, and cannot be configured by the users. The amount of physical memory from the total server memory the virtual machine has allocated in the template file.
Maximum Virtual CPUs	This is a display only field. CPU allocation for the virtual machine from the template file.
CPU Time	The amount of CPU time the virtual machine has had since boot. This is not the same as uptime.
State	Current status of the virtual machine.

Name	Description
	Possible values are as follows: • **Running**: Virtual machine is running normally. • **Starting**: Virtual machine is currently booting and should enter a running state when complete. • **Stopping**: Virtual machine is in the process of being shutdown and should enter stopped state when complete. • **Stopped**: Virtual machine has been shutdown. • **Rebooting**: Virtual machine is in the process of a reboot and should return to running when complete. • **No State**: The virtual machine is not running or the application watchdog is not being used. • **N/A**: The normal state applicable for System Domain and Console Domain virtual machines.
Application State	Current status of the application (respective virtual machine). Possible values are as follows: • **Starting**: Application is currently booting and should enter a running state when complete. • **Running**: Application is running normally. • **Stopped**: Application has been shutdown. • **Stopping**: Application is in the process of being shutdown and should enter stopped state when complete. • **Partial**: Some elements of the application are running, but not all elements. • **Timeout**: Application has missed a heartbeat, signifying a problem and may result in the Console Domain rebooting the virtual machine to clear the problem.

Name	Description
	• **Error**: Application's sanity mechanism provided some kind of error message. • **Unknown**: Application's sanity mechanism failed.

Button descriptions

Name	Description
Refresh	Refreshes the list of virtual machines.

Related topics:

Viewing virtual machines on page 567
Rebooting a virtual machine on page 568
Shutting down a virtual machine on page 568

Virtual Machine Configuration Parameters field descriptions

Use the Virtual Machine Configuration Parameters page to view details for a virtual machine or to reboot or shut down a virtual machine.

Name	Description
Name	Name of the virtual machines running on System Platform.
MAC Address	Machine address of the virtual machine.
IP Address	IP address of the virtual machine.
OS Type	Operating system of the virtual machine, for example, Linux or Windows.
State	Current status of the virtual machine. Possible values are as follows: • **Running**: Virtual machine is running normally. • **Starting**: Virtual machine is currently booting and should enter a running state when complete. • **Stopping**: Virtual machine is in the process of being shutdown and should enter stopped state when complete.

Name	Description
	• **Stopped**: Virtual machine has been shutdown. • **Rebooting**: Virtual machine is in the process of a reboot and should return to running when complete. • **No State**: The virtual machine is not running or the application watchdog is not being used.
Application State	State of virtual machine as communicated by the watchdog. A virtual machine may include an application watchdog. This watchdog communicates application health back to the Console Domain. Current status of the application (respective virtual machine). Possible values are as follows: • **Starting**: Virtual machine is currently booting and should enter a running state when complete. • **Running**: Virtual machine is running normally. • **Stopped**: Virtual machine has been shutdown. • **Stopping**: Virtual machine is in the process of shutting down and should enter stopped state when complete. • **Partial** : Some elements of the virtual machine are running, but not all elements. • **Timeout**: Virtual machine has missed a heartbeat, signifying a problem and may result in the Console Domain rebooting the virtual machine to clear the problem. • **Error**: Virtual machine's sanity mechanism provided some kind of error message. • **Unknown**: Virtual machine's sanity mechanism failed.
Used Memory	The amount of memory currently used by the virtual machine.

Name	Description
Maximum Memory	The amount of physical memory from the total server memory the virtual machine has allocated in the template file. This is a display only field.
CPU Time	The amount of CPU time the virtual machine has had since boot. This is not the same as uptime.
Virtual CPUs	The maximum number of virtual CPUs used by the respective virtual machine.
Domain UUID	Unique ID of the virtual machine.
Auto Start	Status of auto start of a virtual machine: if the virtual machine starts automatically after a shut down operation. Available status are **True** (if auto start is set), and **False** (if auto start is not set). ✱ **Note:** This value should be changed only for troubleshooting purposes.

Button descriptions

Button	Description
Reboot	Reboots the respective virtual machine. In the case of System Domain (Domain-0), this reboot operation is the same as the reboot operation available in the left navigation pane. When you reboot the System Platform server using the reboot option in the left navigation pane, the system shuts down the System Platform server and all the virtual machines running on it. ! **Important:** When you reboot System Domain (Domain-0), the system reboots the System Platform server and all the virtual machines running on it, causing potential service disruption. When you reboot Console Domain, the system loses connection with the System Platform Web Console. You can log in again after Console Domain finishes the reboot operation.

Button	Description
Shutdown Server	Appears only if **Domain-0** is selected and shuts down the server and all virtual machines running on it.
Stop	Appears if a virtual machine other than System Domain (Domain-0) or Console Domain is selected and stops the selected virtual machine.
Start	Appears if a virtual machine other than System Domain (Domain-0) or Console Domain is selected and starts the selected virtual machine.

Related topics:

Viewing virtual machines on page 567
Rebooting a virtual machine on page 568
Shutting down a virtual machine on page 568

Deleting a solution template

About this task

This procedure deletes all applications (virtual machines) in the solution template that is installed.

Procedure

1. Click **Virtual Machine Mangement** > **Solution Template**.
2. On the Search Local and Remote Template page, click **Delete Installed Template**.
3. Click **Ok** to confirm deletion or **Cancel** to cancel deletion.

Chapter 21: Server management

Server Management overview

Use the options under Server Management to perform various administrative activities for the System Platform server. Some of the administrative activities that you can perform include:

- Configuring various settings for the server
- Viewing log files
- Upgrading to a latest release of the software
- Backing up and restoring current version of the software

Managing patches

Patch management

You can install, download, and manage the regular updates and patches for System Platform and the various templates provided by Avaya. Go to http://support.avaya.com and see the latest Release Notes for information about the latest patches.

You can install or download the patches from the Avaya Product Licensing and Delivery System (PLDS) Web site at http://plds.avaya.com.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:

- **Avaya Downloads (PLDS)**
- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Related topics:

Configuring a proxy on page 576
Search Local and Remote Patch field descriptions on page 578

Configuring a proxy

About this task

If the patches are located in a different server (for example, Avaya PLDS or HTTP), you may need to configure a proxy depending on your network.

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Upload/Download**.
3. On the Search Local and Remote Patch page, click **Configure Proxy**.
4. On the System Configuration page, select **Enabled** for the **Proxy Status** field.
5. Specify the proxy address.
6. Specify the proxy port.
7. Select the appropriate keyboard layout.
8. Enable or disable statistics collection.
9. Click **Save** to save the settings and configure the proxy.

Related topics:

Search Local and Remote Patch field descriptions on page 578

System configuration field descriptions on page 591

Installing patches

About this task

Use this task to install all patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

Procedure

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Related topics:

Patch List field descriptions on page 580

Patch Detail field descriptions on page 580

Removing patches

Procedure

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch that you want to remove.
4. On the Patch Detail page, click **Deactivate**, if you are removing a template patch.
5. Click **Remove**.

Tip:

You can clean up the hard disk of your system by removing a patch installation file that is not installed. To do so, in the last step, click **Remove Patch File**.

Related topics:

Patch List field descriptions on page 580
Patch Detail field descriptions on page 580

Search Local and Remote Patch field descriptions

Use the Search Local and Remote Patch page to search for available patches and to upload or download a patch.

Name	Description
Supported Patch File Extensions	The patch that you are installing should match the extensions in this list. For example, *.tar.gz,*.tar.bz,*.gz,*.bz,*.zip,*.tar,*.jar,*.rpm,*.patch.
Choose Media	Displays the available location options for searching a patch. Options are: • **Avaya Downloads (PLDS)**: The template files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password. The list will contain all the templates to which your company is entitled. Each line in the list begins with the "sold-to" number to allow you to select the appropriate template for the site where you are installing. You may hold the mouse pointer over the selection to view more information about the "sold-to" number. • **HTTP**: Files are located in a different server. You must specify the Patch URL for the server. • **SP Server**: Files are located in the vsp-template file system in the System Platform server. You must specify the Patch URL for the server. **Tip:** When you want to move files from your laptop to the System Platform Server,

Name	Description
	you may encounter some errors, as System Domain (Dom–0) and Console Domain support only SCP, but most laptops do not come with SCP support. You can download the following two programs to enable SCP (Search on the Internet for detailed procedures to download them): - Pscp.exe - WinSCP • **SP CD/DVD**: Files are located in a System Platform CD or DVD. • **SP USB Disk**: Files are located in a USB flash drive. • **Local File System**: Files are located in a local computer.
Patch URL	Active only when you select **HTTP** or **SP Server** as the media location. URL of the server where the patch files are located.

Button descriptions

Button	Description
Search	Searches for the available patches in the media location you specify.
Configure Proxy	Active only when you select **HTTP** as the media location option. Opens the System Configuration page and lets you configure a proxy based on your specifications. If the patches are located in a different server, you may be required to configure a proxy depending on your network.
Add	Appears when **Local File System** is selected and adds a patch file to the local file system.
Upload	Appears when **Local File System** is selected and uploads a patch file from the local file system.
Download	Downloads a patch file.

Related topics:

Downloading patches on page 575

Configuring a proxy on page 576

Patch List field descriptions

The Patch List page displays the patches on the System Platform server for installing or removing. Use this page to view the details of patch file by clicking on the file name.

Name	Description
System Platform	Lists the patches available for System Platform under this heading.
Solution Template	Lists the patches available for the respective solution templates under respective solution template headings.
Patch ID	File name of a patch.
Description	Information of a patch, for example, if the patch is available for System Platform the description is shown as SP patch.
Status	Shows the status of a patch. Possible values of **Status** are **Installed**, **Not Installed**, **Active**, and **Not Activated**.
Service Effecting	Shows if installing the patch causes the respective virtual machine to reboot.

Button descriptions

Button	Description
Refresh	Refreshes the patch list.

Related topics:

Installing patches on page 577

Removing patches on page 577

Patch Detail field descriptions

The Patch Detail page provides detailed information about a patch. Use this page to view details of a patch or to install or remove a patch.

Name	Description
ID	File name of the patch file.
Version	Version of the patch file.
Product ID	Name of the virtual machine.
Description	Virtual machine name for which the patch is applicable.
Detail	Virtual machine name for which the patch is applicable. For example, Console Domain (cdom patch).
Dependency	Shows if the patch file has any dependency on any other file.
Applicable for	Shows the software load for which the patch is applicable.
Service effecting when	Shows the action (if any) that causes the selected patch to restart the System Platform Web Console.
Disable sanity when	Shows at what stage the sanity is set to disable.
Status	Shows if the patch is available for installing or already installed.
Patch File	Shows the URL for the patch file.

Button descriptions

Button	Description
Refresh	Refreshes the Patch Details page.
Patch List	Opens the Patch List page, that displays the list of patches.
Install	Installs the respective patch.
Activate	Activates the installed patch of a solution template.
Deactivate	Deactivates the installed patch of a solution template.
Remove	Removes the respective patch.
Remove Patch File	Removes the respective patch file. The button appears only if the patch file is still present in the system. On removing the patch file, the button does not appear.

Related topics:

Installing patches on page 577
Removing patches on page 577

Viewing System Platform logs

Log viewer

You can use the Log Viewer page to view the following log files that System Platform generates:

- System logs: These logs contain the messages that the System Platform operating system generates.
- Event logs: These logs contain the messages that the System Platform generates.
- Audit logs: These logs contain the messages that the System Platform generates as a record of user interaction such as the action performed, the time when the action was performed, the user who performed the action, and so on.

To view a log, you should provide the following specifications:

- Select one of the following logs to view:
    - System logs
    - Event logs
    - Audit logs
- Select one of the log levels relevant to the selected logs. The log level denotes the type of incident that might have occurred such as an alert, an error condition, a warning, or a notice.
- Specify a time duration within which an incident of the selected log level might have occurred.
- Enter some text that you want to search in the selected logs. This is optional.

Viewing log files

Procedure

1. Click **Server Management** > **Log Viewer**.
2. On the Log Viewer page, do one of the following to view log files:

- Select a message area and a log level area from the list of options.
- Enter text to find a log.

3. Click **Search**.

Related topics:
Log Viewer field descriptions on page 583

Log Viewer field descriptions

Use the Log Viewer page to view various log messages that the system has generated.

Name	Description
Messages	Select the type of log messages that you want to view. Options are: • **System Logs** are log messages generated by the System Platform operating system (syslog). • **Event Logs** are log messages generated by the System Platform software. These logs are related to processes and commands that have run on System Platform. • **Audit Logs** are a history of commands that users have run on the platform.
Log Levels	Select the severity of log messages that you want to view: Options are: • **Alert** • **Critical/Fatal** • **Error** • **Warning** • **Notice** • **Informational** • **Debug/Fine** If you select **Audit Logs** for **Messages**, you have only **Informational** as an option.
Timestamp From	The timestamp of the last message in the type of log messages selected.

Name	Description
	This timestamp is greater than or equal to the value entered for **Timestamp From**.
To	The timestamp of the first message in the type of log messages selected. This timestamp is less than or equal to the value entered for **To**.
Find	Lets you search for particular log messages or log levels.

Button descriptions

Button	Description
Search	Searches for the log messages based on your selection of message category and log levels.

Related topics:

Viewing log files on page 582

Log severity levels on page 588

Configuring date and time

Configuring System Platform to synchronize with an NTP server

About this task

Configuring the date and time are optional and you can skip these steps. However, you must set up the correct time zone for System Platform.

Procedure

1. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page with default configuration settings.

2. Specify a time server and click **Add** to add the time server to the configuration file.

3. Click **Ping** to check whether the specified time server, that is, the specified host, is reachable across the network.

4. Click **Start ntpd** to synchronize the System Platform time with the Network Time Protocol (NTP) server.

   If you want to stop the synchronization, click the same button, which the system now displays as **Stop ntpd**.
5. Select a time zone and click **Set Time Zone** to set the time zone in System Platform.
   The system sets the selected time zone on the System Platform virtual machines (System Domain (Dom-0) and Console Domain). The system also updates the time zone on the other virtual machines.
6. Click **Query State** to check the NTP (Network Time Protocol) status.

Related topics:

NTP daemon on page 586
Date Time Configuration field descriptions on page 587

Configuring date and time

About this task

Use this procedure to configure the date and time if you are not synchronizing the System Platform server with an NTP server.

Configuring the date and time are optional and you can skip these steps. However, you must set up the correct time zone for System Platform.

Procedure

1. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page with default configuration settings.
2. Click the calendar icon located next to the **Save Date and Time** button.

   The system displays the Set Date and Time page.

   Note:

   If the **Save Date and Time** button is not enabled, you must stop the NTP server that is currently being used.
3. Select a date in the calendar to change the default date and set the required date.
4. Do the following to set the time:
   a. Click the time field at the bottom of the calendar.
      The system displays a box showing time information.

   b. Use the up and down arrow keys beside the hour to change the hour, and up and down arrows beside the minutes field to set the minutes.
   c. Click **OK** to accept your time changes.

5. Click **Apply** to save your changes.
6. Click **Save Date and Time**.
   The system displays a warning message stating that this action will cause a full system reboot.
7. Click **OK** to accept the message and set the updated date and time in the system.

Related topics:
Date Time Configuration field descriptions on page 587

NTP daemon

The NTP daemon reads its configuration from a file named ntp.conf. The ntp.conf file contains at least one or more lines starting with the keyword *server*. Each of those lines specify one reference time source, that is, time server, which can be either another computer on the network, or a clock connected to the local computer.

Reference time sources are specified using IP addresses, or host names which can be resolved by a name server. NTP uses the pseudo IP address 127.127.1.0 to access its own system clock, also known as the local clock. You must not mix this IP address with 127.0.0.1, which is the IP address of the local host, that is the computer's loopback interface. The local clock will be used as a fallback resource if no other time source is available. That is why the system does not allow you to remove the local clock.

Related topics:
Configuring System Platform to synchronize with an NTP server on page 584
Date Time Configuration field descriptions on page 587

Removing a time server

Procedure

1. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page.
2. Select a time server from the list of added servers and click **Remove Time Server** to remove the selected time server.

Note:

The changes will be effective after you restart NTP.

Related topics:

Date Time Configuration field descriptions on page 587

Date Time Configuration field descriptions

Use the Date/Time Configuration page to view or change the current date, time, time zone, or the status of NTP daemon on the System Platform server.

Name	Description
Date/Time Configuration	Shows the local time and the UTC time. Also shows the status of the NTP daemon, if it is started or stopped.
Save Date and Time	Lets you edit the date and time set during System Platform installation.
Manage Time Servers	Lets you ping a time server and see its status and manage the existing time servers.

Button descriptions

Button	Description
Start ntpd	Starts the Network Time Protocol (NTP) daemon on System Platform to synchronize the server time with an NTP server. If the NTP daemon (ntpd) is started, this button changes to **Stop ntpd**. Click this button to stop the NTP daemon.
Set Date and Time	Edits the date and time that are configured for System Platform. The button is disabled if ntpd is running.
Set Time Zone	Edits the time zone that is configured for System Platform . System Platform updates the time zone on System Domain (Domain-0), Console Domain, and the virtual machines running on System Platform.
Ping	Checks whether the specified time server, that is, the specified host, is reachable across the network.

Button	Description
Add	Adds the time server that you specify to the list of time servers with which System Platform can synchronize.
Remove Time Server	Removes the selected time server.
Query State	Checks the status of the NTP daemon on System Platform.

Related topics:

Configuring System Platform to synchronize with an NTP server on page 584
Configuring date and time on page 585
NTP daemon on page 586
Removing a time server on page 586

Configuring Logging

Log severity levels

Different log messages in System Platform have different severity levels. The severity levels are:

- Fine
- Informational
- Warning
- Error
- Fatal

You can select how detailed the log output of System Platform will be. Log messages of the severity you select and of all higher severities are logged. For example, if you select Information, log messages of severity levels Information, Warning, Error, and Fatal are logged. Log messages of severity level Fine are not logged.

Log retention

To control the size and number of historical log files that System Platform retains, you configure a maximum size for log files and a maximum number of log files.

When a log file reaches the maximum size, it rolls over. When rollover occurs, .1 is appended to the file name of the current log file and a new, empty log file is created with the original name. For example, `vsp-all.log` is renamed `vsp-all.log.1`, and a new, empty `vsp-`

`all.log` file is created. The number that is appended to older log files is increased by one. For example, the previous `vsp-all.log.1` is renamed `vsp-all.log.2`, `vsp-all.log.2` is renamed `vsp-all.log.3`, and so on. When the maximum number of backup (old) log files is reached, the oldest log file is deleted.

Configuring log levels and retention parameters

Procedure

1. Click **Server Management** > **Logging Configuration**.
2. Edit the default values, if required.
3. Click **Save** to save the settings.

Related topics:

Log severity levels on page 588
Log retention on page 588
Logging Configuration field descriptions on page 589

Logging Configuration field descriptions

Use the Logging Configuration page to configure the severity of log messages that you want logged, a maximum size for log files, and the number of backup files that you want retained.

⚠ **Caution:**

Change the default values only for troubleshooting purposes. If you change the logger level to **FINE**, the system writes many log files. There are chances of potential performance issues when using this logging level. So, Avaya recommends you to switch to **FINE** only to debug a serious issue.

Name	Description
SP Logger	SP Logger is used for the System Platform Web Console logs, which are generated by the System Platform code base (for example, com.avaya.vsp).
3rd Party Logger	Third Party Logger is the root logger, which can include logs from other third party components included in the System Platform Web Console (for example, com.* or com.apache.*).

Name	Description
vsp-all.log	Contains all logs generated bySystem Platform Web Console, regardless of whether they include event codes.
vsp-event.log	Contains all event logs generated by System Platform Web Console. The logs in vsp-event are available in Avaya common logging format.
vsp-rsyslog.log	Contains syslog messages.
Max Backups	Maximum number of historical files to keep for the specified log file.
Max FileSize	Maximum file size (for example, for a file vsp-all.log. Once the maximum file size is reached it, the log file will roll over (be renamed) to vsp-all.log.1.

Related topics:

Log severity levels on page 588

Log retention on page 588

Configuring log levels and retention parameters on page 589

Configuring the system

Configuring system settings for System Platform

Procedure

1. Click **Server Management** > **System Configuration**.
2. On the System Configuration page, modify the fields as appropriate. If the default settings are satisfactory, no changes are necessary.
3. Click **Save**.

Related topics:

System configuration field descriptions on page 591

System configuration field descriptions

Use the System Configuration page to configure proxy settings, change the current keyboard layout, or enable or disable statistics collection.

Name	Description
Proxy Status	Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform.
Proxy Address	The address for the proxy server.
Proxy Port	The port address for the proxy server.
Keyboard Layout	Determines the specified keyboard layout for the keyboard attached to the System Platform server.
Statistics Collection	If you disable this option, the system stops collecting the statistics data. **Note:** If you stop collecting statistics, the system-generated alarms will be disabled automatically.

Related topics:

Configuring system settings for System Platform on page 590

Configuring network settings

Configuring System Platform network settings

About this task

Important:

The System Platform network settings are independent of the network settings of the virtual machines running on it. This means that the System Platform network settings will not affect the network settings of the virtual machines.

Make sure that the IP addresses for the *avprivate* bridge do not conflict with any other IP addresses in your network.

The Network Configuration page displays the addresses that are allocated to avprivate. The range of IP addresses starts with System Domain's (Dom-0) interface on avprivate. If any conflicts exist, resolve them. Keep in mind that the template you install may take additional addresses on the private bridge.

The avprivate bridge is an internal, private bridge that allows virtual machines to communicate with each other. This private bridge does not have any connection to your LAN. During installation, System Platform runs an algorithm to find a set of IP addresses that do not conflict with the addresses configured on the System Domain Network Configuration page. However, it is still possible that the addresses selected conflict with other addresses in your network. Since this private bridge is not connected to your LAN, this address conflict could result in the failure of System Platform or an installed template to route packets correctly.

Important:

Avaya recommends that you change all the IP addresses (wherever required) in a single instance to minimize the service disruption.

Procedure

1. Click **Server Management** > **Network Configuration**.
2. On the Network Configuration page enter values to configure the network settings.
3. Click **Save**.

Related topics:

Network Configuration field descriptions on page 592

Network Configuration field descriptions

Use the **Network Configuration** page to configure network settings for System Platform. The first time that you view this page, it displays the network settings that you configured during installation of System Platform.

After you install a template, the Network Configuration page displays additional fields based on the specific template installed. Examples of template-specific fields include bridges, dedicated NICs, or IP configuration for each of the guest domains created for the template.

The bonding interface fields explained below are applicable only to certain templates such as Duplex Survivable Core.

Enable IPv6 field description

Name	Description
Turn On IPv6	Enables IPv6.

General Network Settings field descriptions

Name	Description
Default Gateway	The default gateway.
Primary DNS	The primary DNS server address.
Secondary DNS	(Optional) The secondary DNS server address.
Domain Search List	The search list, which is normally determined from the local domain name. By default, it contains only the local domain name. This may be changed by listing the desired domain search path following the *search* keyword with spaces or tabs separating the names.
Udom hostname	The host name for the Console Domain. This must be a fully qualified domain name (FQDN), for example, SPCdom.mydomainname.com.
Dom0 hostname	The host name for System Domain (Domain-0). This must be a fully qualified domain name (FQDN), for example, SPDom0.mydomainname.com.
Physical Network Interface	The physical network interface details for eth0 and eth1 (and eth2 in case of High Availability Failover is enabled).
Domain Dedicated NIC	Applications with high network traffic or time-sensitive traffic may be allocated a dedicated NIC. This means the virtual machine connects directly to a physical Ethernet port and may require a separate cable connection to the customer network. See respective template installation topics for more information.
Bridge	The bridge details for the following: • **avprivate**: This is called a private bridge because it does not use any Ethernet interface, so it is strictly internal to the server. The System Platform installer attempts to assign IP addresses that are not in use. • **avpublic**: This bridge uses the Ethernet interface associated with the default route, which is usually eth0, but can vary based on the type of the server. This bridge

Name	Description
	generally provides access to the LAN for System Platform elements (System Domain (Dom-0) and Console Domain) and for any guest domains that are created when installing a template. The IP addresses specified during System Platform installation are assigned to the interfaces that System Domain (Dom-0) and Console Domain have on this bridge. • **template bridge**: These bridges are created during the template installation and are specific to the virtual machines installed.
Domain Network Interface	The domain network interface details for System Domain (Dom-0) or Console Domain that are grouped by domain based on your selection.
Global Template Network Configuration	The set of IP addresses and host names of the applications hosted on System Platform. Also includes the gateway address and network mask.

Bonding Interface field descriptions

Name	Description
Name	Is a valid bond name. It should match regular expression in the form of “bond[0-9]+”.
Mode	Is a list of available bonding modes that are supported by Linux. The available modes are: • Round Robin • Active/Backup • XOR Policy • Broadcast • IEEE 802.3ad • Adaptive Transmit Load Balancing • Adaptive Load Balance For more information about bonding modes, refer to http://www.linuxhorizon.ro/bonding.html.

Name	Description
	Note: The default mode of new bonding interface is Active/Backup. **Important:** System Platform doesn't allow to configure any advance parameters not listed in this page. If you want to configure an advanced feature, log in to System Platform Web Console and make the required changes.
Slave 1/ Primary	Is the first NIC to be enslaved by the bonding interface. If the mode is Active/Backup, this will be the primary NIC.
Slave 2/Secondary	Is the second NIC to be enslaved by the bonding interface. If the mode is Active/Backup, this will be the secondary NIC.

Bonding Interface link descriptions

Name	Description
Add Bond	Adds new bonding interface.
Delete	Deletes a bonding interface.

Related topics:

Configuring System Platform network settings on page 591

Adding a bonding interface

About this task

While you are configuring network settings in the Network Configuration page, use this procedure to add a bonding interface.

Procedure

1. Scroll down to make the Bonding Interface frame visible.
2. Click **Add Bond** link.
3. Enter the following fields:

a. **Name**
b. **Mode**
c. **Slave 1/Primary**
d. **Slave 2/Primary**

Deleting a bonding interface

About this task

While you are configuring network settings in the Network Configuration page, use this procedure to delete a bonding interface.

Procedure

1. Scroll down to make the Bonding Interface frame visible.
2. Click **Delete** link against the bonding interface you want to delete.

Configuring static routes

Adding a static route

About this task

Use this procedure to add a static route to System Platform. Static routes can be used to route packets through a VPN to an Avaya Partner that is providing remote service.

Procedure

1. Click **Server Management** > **Static Route Configuration**.
2. On the Static Route Configuration page, select the required interface.
3. Enter the network address.
4. Enter the network mask address.
5. Enter the gateway address.
6. Click **Add Route**.

Related topics:

Static route configuration field descriptions on page 597

Deleting a static route

Procedure

1. Click **Server Management** > **Static Route Configuration**.
2. Click **Delete** next to the static route that you want to delete.

Related topics:

Static route configuration field descriptions on page 597

Modifying a static route

About this task

Procedure

1. Click **Server Management** > **Static Route Configuration**.
2. Click **Edit** next to the static route that you want to modify.
3. Modify the settings as appropriate.
4. Click **Apply** to save the settings.

Related topics:

Static route configuration field descriptions on page 597

Static route configuration field descriptions

Use the Static Route Configuration page to add static routes to System Domain (Dom-0), view details of existing static routes, or modify or delete existing static routes.

Field Names	Descriptions
Interface	The bridge through which the route is enabled.
Network Address	The destination network for the static route.

Field Names	Descriptions
Network Mask	The network mask for the destination network.
Gateway	The gateway or the router through which the route functions.

Related topics:

Adding a static route on page 596
Deleting a static route on page 597
Modifying a static route on page 597

Configuring Ethernet settings

Configuring Ethernet interface settings

Procedure

1. Click **Server Management** > **Ethernet Configuration**.

   The Ethernet Configuration page displays the values for all Ethernet interfaces on the server, for example, eth0, eth1, eth2, and so on.
2. Modify the values for eth0 and eth1 as appropriate.
3. Click **Save** to save your settings.

Related topics:

Ethernet configuration field descriptions on page 598

Ethernet configuration field descriptions

Use the Ethernet Configuration page to configure settings for the Ethernet interfaces on System Platform.

Name	Description
Speed	Sets the speed in MB per second for the interface. Options are: • 10 Mb/s half duplex • 10 Mb/s full duplex • 100 Mb/s half duplex • 100 Mb/s full duplex • 1000 Mb/s full duplex Auto-Negotiation must be disabled to configure this field.
Port	Lists the available Ethernet ports. Auto-Negotiation must be disabled to configure this field.
Auto-Negotiation	Enables or disables auto-negotiation. By default it is enabled, but might cause some problems with some network devices. In such cases you can disable this option.

Button descriptions

Button	Description
Apply	Saves and applies the settings for the Ethernet device.
Refresh	Refreshes the Ethernet Configuration page.

Related topics:

Configuring Ethernet interface settings on page 598

Configuring alarms

Alarm descriptions

System Platform generates the following alarms:

Alarm	Description
High CPU	Average CPU Usage of VM

Alarm	Description
Disk Usage (Logical Volume)	Percentage of logical volume used (/, /template-env, /dev/shm, /vspdata, vsp-template)
Disk (Volume Group)	Percentage of volume group used (VolGroup00)
Disk reads	Disk read rate (sda)
Disk Writes	Disk write rate (sda)
Load Average	Load average on each virtual machine
Network I/O received	Network receive rate for all guests (excluding dedicated NICs)
Network I/O Transmit	Network transmit rate for all guests (excluding dedicated NICs)
Webconsole heap	Percentage of webconsole (tomcat) heap memory in use
Webconsole open files	Number of file descriptors that webconsole has open
Webconsole permgen	Percentage of webconsole (tomcat) permgen heap used
SAL Agent heap SAL Agent permgen	Percentage of SAL heap memory in use
SAL Agent permgen	Percentage of SAL permgen heap used
Domain-0 Memory (Committed_AS)	Memory for System Domain (Dom-0)
udom Memory (Committed_AS)	Memory for Console Domain

Note:

A virtual machine other than System Domain and Console Domain may support configuring alarms relevant to its operations. Please check the administration document of the virtual machine to know whether any alarms are present for the virtual machine and how to configure them.

Configuring alarm settings

Procedure

1. Click **Server Management** > **Alarm Configuration**.
2. On the Alarm Configuration page, modify the settings as appropriate.
3. Select **Enabled** to enable an alarm.

4. In the **Limit Value** field, enter the threshold value for the alarm.
5. Specify the number of consecutive samples that must exceed the threshold value for the system to generate an alarm.
6. Specify the **Suppression Period** for an alarm after the system generates the previous alarm.
7. Click **Save** to save the settings.

Related topics:

Alarm descriptions on page 599

Alarm configuration field descriptions on page 601

Alarm configuration field descriptions

Use the **Alarm Configuration** page to configure alarms generated from the data collected by the Performance Statistics feature.

Field Names	Descriptions
Alarm	Name of the alarm.
Limit Values	The threshold value above which the value is potentially in an alarming state.
For	The period for which the value must be above the threshold to generate an alarm.
Suppression Period	The period for which the same alarm is not repeated after generating the alarm for the first time.
Enable	Enables the selected alarm.

Related topics:

Alarm descriptions on page 599

Configuring alarm settings on page 600

Managing Certificates

Certificate management

The certificate management feature allows a user with the right administrative privileges to replace the default System Platform Web Console certificate and private key. It also allows the user to upload and replace the enterprise LDAP certificate, if the option of transport layer security (TLS) was enabled in the Enterprise LDAP page.

The user can replace the default System Platform Web Console certificate and private key by selecting a new certificate file and a new private key on the local machine and uploading them. The default System Platform Web Console certificate is generated during System Platform installation with the CN value same as the Console Domain hostname. During platform upgrade, the certificate is first backed up and then restored after the upgrade completes.

Similarly, the user can upload and replace the enterprise LDAP certificate by selecting new certificate file on the local machine, and uploading it. The Certificate Management page shows the following data for the current System Platform Web Console and Enterprise LDAP certificate:

- Type
- Version
- Expiry date
- Issuer

Here are the things to note relating to a certificate:

- The only acceptable extension of a new certificate file is `.crt`.
- The only acceptable extension of a new private key file is `.key`.
- The option to upload the key is only for the System Platform Web Console certificate.
- An uploaded certificate is valid if its start date is not after the current date and its end date is not before the current date. An uploaded private key is valid if it matches the uploaded certificate.

Related topics:

Enterprise LDAP field descriptions on page 635

Selecting System Platform certificate

Procedure

1. Click **Server Management** > **Certificate Management**.
2. Click **Select New Certificate** in the System Platform Certificate area.

Selecting enterprise LDAP certificate

About this task

This task is enabled only if **TLS** was clicked in the Enterprise LDAP page.

Procedure

1. Click **Server Management** > **Certificate Management**.
2. Click **Select New Certificate** in the Enterprise LDAP Certificate area.

Related topics:

Configuring authentication against an enterprise LDAP on page 634

Certificate Management field descriptions

Use the Certificate Management page to get new certificate issued from your certification authority for System Platform Web Console or Enterprise LDAP. In the case of System Platform Web Console, you also get the private key.

Field descriptions

Name	Description
Type	Is the type of the certificate issued.
Version	Is the version number of the certificate.
Expiry Date	Is the expiry date of the certificate.
Issuer	Is the issuing agency of the certificate.

Button descriptions

Name	Description
Select New Certificate	Selects new System Platform Web Console certificate and private key or Enterprise LDAP certificate depending on the area where the button is located.

Managing System Platform licenses

License management

System Platform includes Avaya's Web License Manager (WebLM) to manage its licenses. WebLM is a Web-based software application that facilitates easy tracking of licenses. You can launch the WebLM application from within System Platform.

Launching WebLM

About this task

System Platform uses Web License Manager (WebLM) to manage its licenses. Use this procedure to launch WebLM from System Platform.

Procedure

1. Click **Server Management** > **License Management**.
2. On the License Management page, click **Launch WebLM License Manager** .
3. When WebLM displays its Logon page, enter the user name and password for WebLM. For initial login to WebLM, the user name is `admin`, and the password is `weblmadmin`. However, you must change the password the first time that you log in to WebLM.
4. Manage the licenses as appropriate.

   For more information on managing licenses in Avaya WebLM, see *Installing and Configuring Avaya WebLM Server* at http://www.avaya.com/css/P8/documents/100069577.

Related topics:

License management on page 604
License Management field descriptions on page 604

License Management field descriptions

Use the **License Management** page to launch the Web License Manager (WebLM) application and manage System Platform licenses.

Button descriptions

Name	Description
Launch WebLM License Manager	Launches the WebLM application.

Related topics:

License management on page 604
Launching WebLM on page 604

Configuring the SAL Gateway

SAL

System Platform includes Avaya's Secure Access Link (SAL) Gateway to manage service delivery (alarming and remote access). SAL Gateway is a software application that:

- Facilitates remote access to support personnel and tools that are needed to access supported devices
- Collects and sends alarm information to a Secure Access Concentrator Core Server, on behalf of the managed devices
- Provides a user interface to configure its interfaces to managed devices, Concentrator Remote and Core Servers, and other settings

SAL requires an upload bandwidth (customer to Avaya) of at least 90 kB/s (720 kb/s) with latency no greater than 150 ms (round trip.)

During the installation of System Platform, you must register the system (System Platform, solution templates, and SAL Gateway) and configure SAL for the customer's network.

! **Important:**

For Avaya to provide support, Avaya Partners or their customers must ensure that SAL is registered and configured properly. Avaya support will be delayed or not possible if SAL is not properly implemented.

Avaya Partners must provide their own B2B VPN connection (or other IP-based connectivity) to deliver remote services. SAL does not support modem connections.

You can launch the SAL Gateway management portal from within System Platform.

Launching the SAL Gateway management portal

About this task

Use this procedure to launch the SAL Gateway management portal from within System Platform.

Procedure

1. Click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.
3. When the portal displays its Log On page, enter your user name and password for Console Domain.
4. Configure the SAL Gateway as appropriate.

Related topics:

SAL on page 605
Configuring the SAL Gateway on page 606
SAL Gateway Management field descriptions on page 607

Configuring the SAL Gateway

Procedure

To configure the SAL Gateway for the customer's network and System Platform, follow the instructions that are provided in *Administering SAL on Avaya Aura^{TM} System Platform*. This document is available on http://support.avaya.com/css/P8/documents/100069101.

Note:

For an understanding of how to administer the customer's network to support SAL, follow the instructions provided in *Secure Access Link 1.8 SAL Gateway Implementation Guide*. This document is available on http://www.avaya.com/support.

SAL Gateway Management field descriptions

Button	Description
Launch SAL Gateway Management Portal	Launches the SAL Gateway management portal in a new Web browser window. You must provide valid certificate details to access the portal.

Related topics:

SAL on page 605
Launching the SAL Gateway management portal on page 606
Configuring the SAL Gateway on page 606

Viewing System Platform statistics

Performance statistics

System Platform collects data on operational parameters such as CPU usage, free and used heap and permgen memory, number of open files on System Platform Web Console, and disk input and output operations to name a few. System Platform collects this data at one minute interval and stores it in an RDD database. System Platform presents this data as graphs using an open source data logging and graphing tool called RRDtool. The following sections should help you understand the System Platform performance statistics capability:

Data retention and consolidation

System Platform stores data for 24 hours and then consolidates it into one hour average and maximum, which is kept for a week. After a week, System Platform consolidates the one hour average and maximum data into 4 hour average and maximum, and stores it for six months.

Monitored parameters

System Platform collects data on the following parameters every minute:

Variable	Domain	Description	Source
CPU usage	All domains	Average CPU usage. Is calculated from cpuSeconds	`xm list -long`
System Platform Web	cdom	Free and used heap and permgen memory.	JVM

Variable	Domain	Description	Source
Console memory			
System Platform Web Console open files	cdom	Number of open file handles.	`proc <pid>/fd`
Spirit agent memory	cdom	Free and used heap and permgen memory.	JVM (through JMX)
Memory usage	Domain-0, cdom	Committed_AS and kernel.	`/proc/meminfo`
Disk space (logical info)	Domain-0, cdom	Mounted at: /, /template-env, /dev/shm, /vspdata, vsp-template	`df`
Disk space (volume group)	Domain-0	VolGroup00	`vgs`
Disk I/O	Domain-0	Disk read and write rate for sda.	`iostat`
Network I/O	All domains	Network receive/transmit rate for all guests (excluding dedicated NICs.)	`xentop`
Load average	Domain-0, cdom	average load.	`/proc/loadavg`

Graphs

Click **Server Management** > **Performance Statistics** to generate graphs for all or selected parameters and for a specified duration. You can also obtain the comma separated value (CSV) file of the graphed data.

Alarms

System Platform can raise alarms for parameters whose values and frequencies exceed the configured threshold limits.

Related topics:

Log severity levels on page 588
Exporting collected data on page 609
Performance statistics field descriptions on page 609

Viewing performance statistics

Procedure

1. Click **Server Management** > **Performance Statistics**.
2. On the Server Management page, perform one of the following steps:

- Select **All Statistics** to generate a graph for all recorded statistics.
- Clear **All Statistics**, and select the type of graph from the **Type** drop down menu. Then select the required domain from the list in the **Domains** box.

3. Specify the date and time for the period that you want the report to cover.
4. Click **Generate** to generate the performance graph for the system.

Related topics:
Exporting collected data on page 609
Performance statistics field descriptions on page 609

Exporting collected data

About this task

Use this procedure to export to a CSV file the data points that were used to generate a graph.

Procedure

1. Click **Server Management** > **Performance Statistics**.
2. On the Performance Statistics page, select the required details and generate a graph.
3. Click **Download CSV File** for the data you want to export.
4. Click **Save** and specify the location to download the data.

Related topics:
Log severity levels on page 588
Performance statistics on page 607
Performance statistics field descriptions on page 609

Performance statistics field descriptions

Use the **Performance Statistics** page to view the health and usage of the system. The Performance Statistics page displays the performance statistics for System Platform and the hosted virtual machines.

Field Names	Descriptions
All Statistics	If you select this option, the system displays a graph for all the recorded statistics.

Field Names	Descriptions
Type	Appears only if the **All Statistics** check box is cleared. Lets you specify the type of statistics you want to display from a list of options.
Domains	Appears only if the **All Statistics** check box is cleared. Lets you select the virtual machines for which you want to generate the statistics, for example, System Domain (Dom-0) and Console Domain.
Date and Time	Lets you specify the date and time for generating performance statistics from three options as follows: **Predefined Values**: Lets you specify the range of days. **Last**: Lets you specify the day or time. **Between**: Lets you specify the date range.
Generate	Generates the performance statistics of the system based on your specifications.

Related topics:

Viewing performance statistics on page 608

Exporting collected data on page 609

Ejecting the CD or DVD

About this task

Use the Eject CD/DVD page to force open the DVD drive of the System Platform server. The CD or DVD used for installing System Platform and virtual machines ejects automatically after successfully completing the installation or an upgrade . However, if any problem occurs during installation or upgrade, the CD or DVD remains locked in the drive. You can use the **Eject CD/DVD** page to force open the drive and remove the CD or DVD.

The data on the CD or DVD receives no damage because of force opening the drive.

Procedure

1. Click **Server Management** > **Eject CD/DVD**.
2. Click **Eject** on the Eject CD/DVD page to eject the CD or DVD.

Deleting old, unused files

About this task

Use the File Management page to delete old versions of the solution template files and platform upgrade images. However, you cannot delete the files for the currently installed solution templates. System Platform stores solution template files and platform upgrade images in a folder on the system.

Procedure

1. Click **Server Management** > **File Manager**.
2. Select the folder file that you want to delete.
3. Click **Delete**.

Configuring security

Security configuration

Most JITC features are built into the System Platform image and are available after installing System Platform. However, there are some features which need more user input and can be configured from the Security Configuration page. This page allows an advanced administrator user to do the following tasks:

- Remove network debugging tools, namely wireshark from System Platform
- Enable JITC Audit
- Set certain security parameters on the system

Important:

Removing the network debugging tools is irreversible. The tools are removed from System Platform Web Console and the Console Domain.

The **Remove network debugging tools (wireshark)** check box is not enabled once the tools are removed from the system. However, a platform upgrade makes the tools available again and the **Remove network debugging tools (wireshark)** check box is also enabled.

Important:

Enabling audit is also irreversible. The **Enable Audit** check box is not available again after you save the changed security configuration.

Configuring security

About this task

Use this procedure to change one or more security features such as enabling audit, resetting the Grub password, changing host access list, and so on.

Procedure

1. Click **Server Management** > **Security Configuration**.
2. Enter one or more required fields in the Security Configuration page.
3. Click **Save**.

Security Configuration field descriptions

Field descriptions

Name	Description
Remove network debugging tools (wireshark)	Indicates whether or not to remove the network debugging tools. **Important:** Removing the network debugging tools is irreversible. The tools are removed from System Platform Web Console and the Console Domain. A platform upgrade makes the tools available again and the **Remove network debugging tools (wireshark)** check box is also enabled.
Enable Audit	Indicates whether or not the audit is to be enabled. **Important:** Enabling audit is irreversible.
Reset Grub Password	Is the new System Platform Web Console Grub password.

Name	Description
Retype Grub Password	Is the new System Platform Web Console Grub password being retyped for verification.
Verify Dom0 Reset Password	Is the System Platform Web Console root password to reset the System Platform Web Console Grub password.
Cdom Hosts Allow List	Is the list of hosts that can access the Console Domain. ✱ **Note:** The list of hosts is maintained in the `hosts.allow` file at `/etc` on the Console Domain.
Cdom Hosts Deny List	Is the list of hosts that cannot access the Console Domain. ✱ **Note:** The list of hosts is maintained in the `hosts.deny` file at `/etc` on the Console Domain. ❗ **Important:** When JITC is enabled, all that `hosts.deny` has is the entry `ALL:ALL`.
Dom0 Hosts Allow List	Is the list of hosts that can access the System Platform Web Console. ✱ **Note:** The list of hosts is maintained in the `hosts.allow` file at `/etc` on the System Platform Web Console.
Dom0 Hosts Deny List	Is the list of hosts that cannot access the System Platform Web Console. ✱ **Note:** The list of hosts is maintained in the `hosts.deny` file at `/etc` on the System Platform Web Console. ❗ **Important:** When JITC is enabled, all that `hosts.deny` has is the entry `ALL:ALL`.

Name	Description
Login Banner Header	Is the header shown for the login banner.
Login Banner Text	Is the text shown for the login banner.

Button descriptions

Name	Description
Save	Saves the security configuration.

Backing up System Platform

System Platform backup

You can back up configuration information for System Platform and the solution template (all virtual machines). Sets of data are backed up and combined into a larger backup archive. Backup sets are related data items that need to be backed up. When you perform a back up, the system executes all the backup sets. All the backup sets must succeed to produce a backup archive. If any of the backup sets fail, then the system removes the backup archive. The amount of data backed up is dependent on the specific solution template.

The system stores the backup data in the `/vspdata/backup` directory in Console Domain. This is a default location. During an upgrade, the system does not upgrade the `/vspdata` folder, so that you can restore the data, if required. You can change this location and back up the System Platform backup archives to a different directory in System Platform or in an external server. You can also send the backup data to an external e-mail address if the file size is not larger than 10 MB.

If a backup fails, the system automatically redirects you to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup is successful.

Note:

It is not the aim of the backup feature to provide a mechanism to re-enable a failed High Availability Failover node back to High Availability Failover configuration. Follow the instructions in this document on how to re-enable failed High Availability Failover node back to High Availability Failover configuration.

Backing up the system by using the System Platform Web Console

About this task

Use this procedure to back up configuration information for System Platform and the solution template (all virtual machines).

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   ❗ **Important:**

   The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     ✳ **Note:**

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Related topics:

Backup field descriptions on page 617

Scheduling a backup

About this task

Use this procedure to back up System Platform and the solution template on a regular basis. Backups are not scheduled by default on System Platform.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select **Schedule Backup**.
4. Specify the following:
   - **Frequency**
   - **Start Time**
   - **Archives kept on server**.
   - **Backup Method**

     Use this field to copy the backup archive file to a remote server or to send the file to an e-mail address. The file is also stored on the on theSystem Platform server.
5. Click **Schedule Backup**.

Related topics:
Backup field descriptions on page 617

Transferring the Backup Archives to a remote destination

About this task

You can send the backup archive to a mail address or to a remote server by SFTP with using the **Backup Method** option.

Procedure

1. To send the archive by email:
   a. Select the **Email** option as the **Backup Method**.
   b. Specify the **Email Address** and the **Mail Server**.
2. To send the archive to a remote server by SFTP:

a. Select **SFTP** option as the **Backup Method**.
b. Specify the **SFTP Hostname** (or IP Address), Directory to which the archive will be sent and the username and password to log in the server.

Viewing backup history

About this task

Use this procedure to view the last 10 backups executed and their status. If the last backup failed, the system automatically redirects you to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup is successful.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select **Backup History**.
   The system displays the last 10 backups executed with their dates and the status.

Backup field descriptions

Use the Backup page to back up configuration information for System Platform and the solution template (all virtual machines).

Backup Now fields

The following table describes the fields that are displayed if you select **Backup Now** at the top of the Backup page.

Field Names	Descriptions
Backup Method	Select a location to send the backup file: • **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory. • **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • **Email**: Sends the backup archive file to the e-mail address that you specify as well as

Field Names	Descriptions
	stores the file on the System Platform server. Enter the e-mail address and the server address of the recipient.
Backup Now	Starts the backup operation.

Schedule Backup fields

The following table describes the fields that are displayed if you select **Schedule Backup** at the top of the Backup page.

Field Names	Descriptions
Frequency	Select one of the following options: • Daily • Weekly • Monthly
Start Time	The start time for the backup.
Archives kept on the server	The number of backup archives to store on the System Platform server. The default is 10.
Backup Method	Select a location to send the backup file: • **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory. • **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server. Enter the e-mail address and the server address of the recipient.
Schedule Backup	Schedules the backup process.
Cancel Schedule	Cancels an existing backup schedule.

Related topics:

Backing up the system by using the System Platform Web Console on page 615

Scheduling a backup on page 616

Restoring System Platform

Restoring backed up configuration information

About this task

Use this procedure to restore backed up configuration information for System Platform and the Solution Template (all virtual machines).

Note:

The restore operation does not restore the High Availability Failover configuration from the backup file. It is not the aim of the restore feature to re-enable the failed High Availability Failover node back to High Availability Failover configuration. Follow the instructions given in this document on how to re-enable the failed High Availability Failover node back to High Availability Failover configuration. Avaya recommends that you restore the backup configuration before configuring and starting High Availability Failover.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
   The Restore page displays a list of previously backed up archives on the System Platform system.
3. Select an archive file from the list, and then click **Restore** to restore from the selected archive.

   Restoring an archive requires the System Platform Web Console to restart, so you must log in again when the restore operation is completed.

Related topics:

System Platform backup on page 614
Restore field descriptions on page 620

Restore field descriptions

Field Names	Descriptions
Restore from	Select the location of the backup archive file from which you want to restore configuration information. • **Local**: Restores from a file on System Platform. If you select this option, the Restore page displays a list of previously backed up archives on the System Platform system. • **SFTP**: Restores from a file on a remote server. If you select this option, enter the hostname or IP address of the remote server, directory where the archive file is located, and user name and password for the SFTP server. • **Upload**: Restores from a file on your computer.
Archive Filename	Filenames of the backup archive files at the location you specify.
Archive Date	Date that the file was created.
Selection	Select this check box to restore from the archive file.
Restore History	Displays the restore history for the last ten restores. If an error occurred during the last restore, the system directs you to this page after login and continues to display an error message until a restore is successful.

Button descriptions

Button	Description
Search	Displayed if you select **SFTP**. Searches for archive files in the specified directory of the remote server.
Clear Search Result	Clears the list of archive files found on a remote server after an SFTP search.

Related topics:

Restoring backed up configuration information on page 619

Viewing restore history

About this task

Use this procedure to view the last 10 restores executed and their status. If the last restore failed, the system automatically redirects you to the Restore page after login and displays the following message: `Last Restore Failed`. The system continues to display the message until a restore is successful

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
3. On the Restore page, select the **Restore History** option.

Rebooting or shutting down the System Platform server

Rebooting the System Platform Server

About this task

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. When this happens, a service disruption may occur.

Note:

You must have a user role of Advanced Administrator to perform this task.

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Reboot**.

Related topics:

Server Reboot Shutdown field descriptions on page 623

Rebooting the whole High Availability Failover system

About this task

When you reboot the whole High Availability Failover system, the system shuts down all the virtual machines running on the primary server, reboots the standby server, and reboots primary server to prevent failover. When this happens, a service disruption may occur.

Only the users of Advanced Administrator role can perform this task.

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Reboot HA System**.

   Note:

   The **Reboot HA System** button is enabled only if the High Availability Failover system is settled and stable to perform this operation.

Shutting down the System Platform Server

About this task

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. When this happens, a service disruption may occur.

Note:

You must have a user role of Advanced Administrator to perform this task.

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown Server**.

Related topics:

Server Reboot Shutdown field descriptions on page 623

Shutting down the whole High Availability Failover system

About this task

When you shut down the whole High Availability Failover system, the system shuts down all the virtual machines running on the primary server, shuts down the secondary server, and shuts down the primary server to prevent failover. When this happens, a service disruption may occur.

Only the users of Advanced Administrator role can perform this task.

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown HA System**.

   Note:

   The **Shutdown HA System** button is enabled only if the High Availability Failover system is settled and stable to perform this operation.

Server Reboot Shutdown field descriptions

Use the Server Reboot/Shutdown page to reboot or shutdown the System Platform server and all the virtual machines running on it.

Name	Description
Name	Name of the application being shutdown. This is always System Domain (Domain-0).
MAC Address	Machine address of the virtual machine.
IP Address	IP address of the System Platform server.
OS Type	Operating system of the System Platform server, for example, Linux.
State	Current status of the virtual machine. Possible values are as follows: • **Running**: Virtual machine is running normally. • **Starting**: Virtual machine is currently booting and should enter a running state when complete.

Name	Description
	• **Stopping**: Virtual machine is in the process of being shutdown and should enter stopped state when complete. • **Stopped**: Virtual machine has been shutdown. • **Rebooting**: Virtual machine is in the process of a reboot and should return to running when complete. • **No State**: The virtual machine is not running or the application watchdog is not being used.
Application State	Current status of the application (respective virtual machine). Possible values are as follows: • **Starting**: Application is currently booting and should enter a running state when complete. • **Running**: Application is running normally. • **Stopped**: Application has been shutdown. • **Stopping**: Application is in the process of being shutdown and should enter stopped state when complete. • **Partial**: Some elements of the application are running, but not all elements. • **Timeout**: Application has missed a heartbeat, signifying a problem and may result in the Console Domain rebooting the virtual machine to clear the problem. • **Error**: Application's sanity mechanism provided some kind of error message. • **Unknown**: Application's sanity mechanism failed.
Used Memory	The amount of memory currently used by the virtual machine.
Maximum Memory	This is a display only field. The amount of physical memory from the total server memory the virtual machine has allocated in the template file.

Name	Description
CPU Time	The amount of CPU time the virtual machine has had since boot. This is not the same as uptime.
Virtual CPUs	The maximum number of virtual CPUs that can run on System Platform server.
Domain UUID	Unique ID of the virtual machine.
Auto Start	Status of auto start - shows if the System Platform server starts automatically after a shut down operation. Available status are **True** (if auto start is set), and **False** (if auto start is not set).

Button descriptions

Button	Description
Reboot	Reboots the System Platform server and all the virtual machines running on it.
Reboot HA System	Reboots the whole High Availability Failover system that includes the primary and the secondary servers and all the virtual machines running on the primary server.
Shutdown Server	Shuts down the System Platform server and all the virtual machines running on it.
Shutdown HA System	Shuts down the whole High Availability Failover system that includes the primary and the secondary servers and all the virtual machines running on the primary server.

Related topics:

Rebooting the System Platform Server on page 621

Shutting down the System Platform Server on page 622

Chapter 22: User Administration

User Administration overview

Use the options under User Administration to manage user accounts for System Platform. Some of the management activities that you can perform include:

- Viewing existing user accounts for System Platform
- Creating new user accounts
- Modifying existing user accounts
- Changing passwords for existing user accounts

User roles

System Platform users must be assigned a user role. Two user roles are available: Administrator and Advanced Administrator. The following table shows which administrative activities each role can perform.

Administrative activity	Administrator	Advanced Administrator
View list of virtual machines.	Yes	Yes
Reboot or shut down virtual machines.	No	Yes
Install solution template.	No	Yes
Upgrade System Platform.	No	Yes
Perform other administrative activities that are available under **Server Management** in the Web Console. Some of these activities include configuring network settings, viewing log files, and backing up the System Platform configuration.	Yes	Yes
Change own password.	Yes	Yes
Create, modify, or delete System Platform users.	No	Yes

Administrative activity	Administrator	Advanced Administrator
Change the password for the System Platform local LDAP.	No	Yes
Configure authentication of System Platform users against an enterprise LDAP.	No	Yes

Related topics:

Creating users on page 631
Modifying users on page 631

Managing System Platform users

By default, System Platform comes with a local LDAP server which is an OpenLDAP Directory Server installed in System Domain. A System Platform user has one of the following two roles that are defined in the local LDAP server:

- Administrator
- Advanced Administrator

System Platform installation creates two users, namely, `admin` and `cust` in the local LDAP server. These users can login to System Platform Web Console. They can also use the command line login to log in to System Domain and Console Domain. The `admin` user has the role of Advanced Administrator and the `cust` user has the role of Administrator.

You can create new System Platform users in the local LDAP server by using the **Local Management** option in the **User Administration** menu.

You can access the **Local Management** option only with an Advanced Administrator role and can perform the following functions:

- Viewing existing users
- Creating new users
- Modifying existing users
- Changing passwords for existing users
- Deleting existing users
- Changing LDAP Manager password

A user with Administrator role can only change own password.

Access restrictions for Administrator role

A user with Advanced Administrator role has no access restrictions when using System Platform Web Console. However, a user with Administrator role has access restrictions in using System Platform Web Console. The following table summarizes those access restrictions:

Menu	Option	Web page control	Access restriction
Virtual Machine Management	**Solution Template**		Denied
	Manage		Granted
	Manage	**Domain-0** link	Denied clicking the **Reboot** and **Shutdown** buttons
	Manage	**cdom** link	Denied clicking the **Reboot** button
	Manage	***VM*** links	Denied clicking the **Reboot**, **Start**, and **Stop** buttons
	View Install/ Upgrade Log		Denied
Server Management	**Patch Management** > **Download/Upload**		Denied
	Platform Upgrade		Denied
	Log Viewer		Granted
	Date / Time Configuration		Granted
	Loggin Configuration		Denied
	System Configuration		Granted
	Network Configuration		Granted
	Static Route Configuration		Granted
	Ethernet Configuration		Granted
	Alarm Configuration		Granted
	Certificate Management		Granted

Menu	Option	Web page control	Access restriction
	License Management		Granted
	SAL Gateway Management		Granted
	Failover		Denied for the **Configure**, **Delete**, **Start**, **Stop**, **Switchover**, **Update SyncSpeed**, **Pause/ Unpause Sync** buttons.
	Performance Statistics		Granted
	Eject CD / DVD		Granted
	File Manager		Granted
	Security Configuration		Denied
	Backup / Restore > **Backup**		Granted
	Backup / Restore > **Restore**		Denied
	Server Reboot / Shutdown		Denied
User Administration	**Local Management**		Denied
	Change LDAP Password		Denied
	Enterprise LDAP		Denied
	Change Password		Denied
	Authentication File		Denied

Note:

A user created using the **User Administration** menu in System Platform Web Console is stored in the local LDAP server and will not appear in the `/etc/shadow` file.

Creating users

About this task

You must have a user role of Advanced Administrator to perform this task.

Procedure

1. Click **User Administration** > **Local Management**.
2. On the Local Management page, click **Create User**. The Local Management page changes to accept the details of new user.
3. In the **User Id** field, enter a unique user ID.
4. In the **User Password** field, enter a password.

   ✱ **Note:**

   Passwords must be at least six characters long. Avaya recommends using only alphanumeric characters.
5. In the **Confirm Password**, enter the same password.
6. In the **User Role** field, click the user role you want to assign to the user.
7. Click **Save User** to the create the user with the details you have specified.

Related topics:

Local Management field descriptions on page 632

Modifying users

About this task

You must have a user role of Advanced Administrator to perform this task.

✱ **Note:**

The `cust` and `admin` user IDs cannot be modified or deleted.

Procedure

1. Click **User Administration** > **Local Management**.
2. On the Local Management page, select the user whose details you want to modify.
3. Click **Edit User**. The Local Management page displays details for the user.

4. In the **New Password** field, enter a new password.

   Note:

   Passwords must be at least six characters long. Avaya recommends using only alphanumeric characters.

5. In the **Confirm Password**, enter the same password.
6. In the **User Role** field, click the user role you want to assign to the user.
7. Click **Save** to save the edited user details.

Related topics:

Local Management field descriptions on page 632

Deleting users

About this task

You must have a user role of Advanced Administrator to perform this task.

Note:

You can delete the default `cust` and `admin` users using this task. You need to create a user with the user role of Advanced Administrator and log in to System Platform Web Console using the login credentials of the new user.

Procedure

1. Click **User Administration** > **Local Management**.
2. On the Local Management page, select the user that you want to delete:
3. Click **Delete User**.
4. In the dialog box that appears to confirm deleting the user, click **OK**.

Related topics:

Local Management field descriptions on page 632

Local Management field descriptions

Use the Local Management page to view, create, modify, or delete user accounts for System Platform.

Manage Users

Name	Description
User Id	User name for the user.
User Role	Role of the user. Options are: • Advanced Administrator • Administrator

Create User and Edit User

Name	Description
User Id	User name for the user.
User Password	Password for the respective user. **Note:** Passwords must be at least six characters long. Avaya recommends using only alphanumeric characters.
Confirm Password	Reenter the password for the user.
User Role	Role of the user. Options are: • Advanced Administrator • Administrator

Related topics:

Creating users on page 631
Modifying users on page 631
Deleting users on page 632

Authenticating System Platform users against an enterprise LDAP

Authentication against an enterprise LDAP

You can configure System Platform to authenticate System Platform users against an enterprise LDAP in addition to authenticating against the local System Platform LDAP. If you do so, users can enter either their enterprise user name and password or System Platform user name and password to log in to the System Platform Web Console.

System Platform first attempts to authenticate a user against the Access Security Gateway (ASG), if present. If the login information does not match the ASG, System Platform attempts to authenticate the user against the local LDAP. If the login information does not match the local LDAP, System Platform finally attempts to authenticate the user against the enterprise LDAP.

Note:

You must have a user role of Advanced Administrator to enable or configure user authentication against an enterprise LDAP.

Related topics:

Configuring authentication against an enterprise LDAP on page 634

Configuring authentication against an enterprise LDAP

About this task

Use this procedure to enable and configure authentication of System Platform users against your enterprise LDAP.

Procedure

1. Click **User Administration** > **Enterprise LDAP**.
2. Select **Enable Enterprise LDAP**.
3. Enter the appropriate information.
4. Click **Save Configuration**.
5. If the **TLS** check box was selected, click **Upload Certificate** to replace the existing enterprise LDAP certificate.
6. Click **Test Connection** to check that you are able to connect to the Enterprise LDAP server.

   Note:

   If you selected the **TLS** check box and could successfully connect to the enterprise LDAP server, it means that you could successfully upload the enterprise LDAP certificate.

Related topics:

Selecting enterprise LDAP certificate on page 603
Authentication against an enterprise LDAP on page 633

Enterprise LDAP field descriptions on page 635

Enterprise LDAP field descriptions

Use the Enterprise LDAP page to enable and configure authentication of System Platform users against your enterprise LDAP.

Name	Description
Enable Enterprise LDAP	This check box enables external LDAP authentication. If you save the page without selecting this check box, the system saves the configuration without activating the enterprise LDAP authentication.
TLS	This check box enables to use Transport Layer Security (TLS).
LDAP Server	Is the Host name or IP address of the LDAP server.
User Attribute	Is the LDAP attribute for the user. This is usually **cn** or **uid**.
Port	Is the port number for the LDAP connection. For TLS-based LDAP connection, the default port number is 636. For non-TLS-based LDAP connection, the default port number is 389.
Base DN	Is the distinguished name of the path where the user search will be executed. This is used for connection authentication to the LDAP server. For example, cn=admin,ou=sv,dc=avaya,dc=com. This parameter is used to login to the LDAP server.
User DN	Is the distinguished name of the LDAP user.
User Password	Is the password of the LDAPuser.
Attribute Map	Specifies LDAP filters for the advanced administrator and administrator roles. A simple filter can be *memberOf=admin_Group*. A complex filter can contain multiple criteria such as: *(&(memberOf=vsp-craft)(userstatus=ACTIVE))*.

Name	Description
Advanced Administrator Filter	Specifies the LDAP filter on a user to check if the user has System Platform advanced administrator role. For example, the LDAP filter *(&(memberOf=vsp-craft)(userstatus=ACTIVE))* will filter the active users who are the members of vsp-craft.
Administrator Filter	Specifies the LDAP filter on a user to check if the user has System Platform administrator role. For example, the LDAP filter *(&(memberOf=vsp-admin)(userstatus=ACTIVE))* will filter the active users who are the members of vsp-admin.

Related topics:

Configuring authentication against an enterprise LDAP on page 634

Changing the System Platform LDAP password

About this task

The local LDAP directory stores login and password details for System Platform users. Use the LDAP login and password to log in to the local LDAP directory. This login does not have permissions to access the System Platform Web Console.

Procedure

1. Click **User Administration** > **Change LDAP Password**.
2. Enter the new password.

   ✱ **Note:**

   Passwords must be at least six characters long. Avaya recommends using only alphanumeric characters.
3. Confirm the new password.
4. Click **Save** to save the new password.

Changing your System Platform password

About this task

The Change Password option is available only for local users. Enterprise LDAP users cannot change their passwords from the System Platform Web Console.

Procedure

1. Click **User Administration** > **Change Password**.
2. In the **Old Password** field, enter your current password.
3. In the **New Password** field, enter a new password.

   Note:

   Passwords must be at least six characters long. Avaya recommends using only alphanumeric characters.
4. In the **Confirm Password** field, reenter the new password.
5. Click **Change Password** to change the current password.

Managing the authentication file

Authentication file for ASG

ASG stands for access security gateway. This gateway ensures that Avaya Partners access the customers' enterprise communication solutions in a secure manner. The Avaya Partners use a predetermined user ID while providing service at the customer site. This user ID is challenged by ASG and requires proper response to make the login successful. Only the Avaya Partners are able to respond to the ASG challenge and that their passwords have single-use life.

An important component of this security mechanism is the customer-specific ASG keys that ASG sets. These keys are stored in an authentication file. To enable Avaya Partners to access their system, customers have to download and install the authentic files specially prepared for their sites.

Installing an authentication file

Procedure

1. Click **User Administration** > **Authentication File**.
2. Click **Upload**.
3. In the Choose File to Upload dialog box, find and select the authentication file, and then click **Open**.

   Note:

   To override validation of the AFID and date and time, select **Force load of new file** on the Authentication File page. Select this option if you:

   - need to install an authentication file that has a different unique AFID than the file that is currently installed, or
   - have already installed a new authentication file but need to reinstall the original file

   You do not need to select this option if you are replacing the default authentication file with a unique authentication file.

   ⚠ **Caution:**

   Use caution when selecting the **Force load of new file** option. If you install the wrong authentication file, certificate errors and login issues may occur.

4. Click **Install**.
   The system uploads the selected authentication file and validates the file. The system installs the authentication file if it is valid.

Chapter 23: Communication Manager objects

Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. Through **Communication Manager** you can directly add, edit, view, or delete the Communication Manager objects . These objects are:

Group	**Communication Manager Object**
Call Center	Agents Announcements Audio Group Best Service Routing Holiday Tables Variables Vector Vector Directory Number Vector Routing Table Service Hours Tables
Coverage	Coverage Answer Group Coverage Path Coverage Remote Coverage Time of Day
Endpoints	Alias Endpoint Intra Switch CDR Manage Endpoints Off PBX Endpoint Mapping Site Data Xmobile Configuration
Groups	Group Page Hunt Group Intercom Group Pickup Group Terminating Extension Group Trunk Group
Network	Automatic Alternate Routing Analysis

	Automatic Alternate Routing Digit Conversion Automatic Route Selection Analysis Automatic Route Selection Digit Conversion Automatic Route Selection Toll Data Modules IP Interfaces IP Network Regions Node Names Route Pattern Signaling Groups
Parameters	System Parameters - CDR Options System Parameters - Customer Options System Parameters - Features System Parameters - Security System Parameters - Special Applications
System	Abbreviated Dialing Enhanced Abbreviated Dialing Group Abbreviated Dialing Personal Authorization Code Class of Restriction Class of Service Class of Service Group Dialplan Analysis Dialplan Parameters Feature Access Codes Locations Uniform Dial Plan

Note:

You cannot add, edit or delete Audio Groups, Announcements, Subscribers and COS objects through Element Cut Through.

Related topics:

Adding Communication Manager objects on page 641
Editing Communication Manager objects on page 641
Viewing Communication Manager objects on page 642
Deleting Communication Manager objects on page 642
Filtering Communication Manager objects on page 643

Adding Communication Manager objects

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Select the Communication Manager object to which you want to add.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Select the Communication Manager again from the list of Communication Managers.

   ✱ **Note:**

   Enter the qualifier number in the **Enter Qualifier** field, if applicable.
7. Click **Add**.
   The system displays the Element Cut Through screen where you can enter the attributes of the Communication Manager object you want to add.
8. Click **Enter** to add the Communication Manager object.

   To return to the Communication Manager screen, click **Cancel**.

Editing Communication Manager objects

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Select the Communication Manager object you want to edit.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the group list, select the device you want to edit.
6. Click **Edit**.

The system displays the Element Cut Through screen where you can edit the attributes of the device you have chosen.

7. To save the changes and go back to the Communication Manager screen, click **Enter**.

   To undo the changes and return to the Communication Manager screen, click **Cancel**.

Viewing Communication Manager objects

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Select the Communication Manager object you want to view.
3. Select a Communication Manager from the list of Communication Manager.
4. Click **Show List**.
5. From the group list, select the object you want to view.
6. Click **View**.
   You can view the attributes of the object you have selected in the Element Cut Through screen.
7. To return to the Communication Manager screen, click **Cancel**.

Deleting Communication Manager objects

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Select the Communication Manager object you want to delete.
3. Select a Communication Manager from the list of Communication Managers.
4. Click **Show List**.
5. Select the objects you want to delete from this group.
6. Click **Delete**.

7. Confirm to delete the Communication Manager objects.

Filtering Communication Manager objects

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Select the Communication Manager object you want to filter.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **Filter: Enable** in the group list.
6. Filter the Communication Manager objects according to one or multiple columns.
7. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

   > **Note:**
   >
   > The table displays only those devices that match the filter criteria.

Chapter 24: Endpoints

Endpoint management

In System Manager, you can create and manage endpoints using the **Manage Endpoints** option. You can also view, edit, and delete endpoints. System Manager provides support for the following set types:

Set Type	
IP/SIP Set types	9610SIP/9620SIP/9630SIP/9640SIP/ 9650SIP 9610/9620/9630/9640/9650 1603/1608/1616/16CC 9600SIP 4620SIP 4620SIPCC 4610/4620/4621/4622/4625/4630 4602+ 4612CL H.323
DCP Set types	2402/2410/2420 6402/6402D/6408/6408+/6408D/6408D+/ 6416D+/6424D+ 8403B/8405B/8405B+/8405D/8405D+/ 8410B/8410D/8411B/8411D/8434D 1408 1416
Analog Set types	2500
BRI Set types	WCBRI

Note:

The set types supported varies based on the Communication Manager versions managed.

Adding an endpoint

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
   The system displays the available Endpoints list on the Communication Manager you selected.
5. Click **New**.
6. Select the template based on the set type you want to add.
   The system displays all the sections on the **Add Endpoint** page.
7. Complete the Add Endpoint page and click **Commit** to add the endpoint.

   You must complete the mandatory fields (marked with an asterisk symbol) under the **General options**, **Feature Options**, **Site Data**, **Data Module/Analog Adjunct**, **Abbreviated Call Dialing**, **Enhanced Call Fwd**, **Button Assignment** sections before adding an endpoint.

   > **Note:**
   >
   > To add an endpoint with a non-supported set type, add the endpoint using Element Cut Through. For alias endpoints, you can choose the corresponding Alias set type from the **Template** field. System Manager automatically creates a template for the Alias set types based on the “aliased-to” set type. Alias endpoint templates have names beginning with “Alias”. Before the Alias endpoint type Template appears in the pull-down menu, you have to create an alias set type on the managed Communication Manager. You can then use the template to add an endpoint.

Related topics:

Endpoint / Template field descriptions on page 653

Using Native Name

About this task

To enter the native name, you must use the Input Method Editor (IME) application. The IME application lets you enter characters in multiple languages such as Japanese, Korean, Russian, Arabic and Chinese without requiring a special keyboard. However, you must enable the IME application manually. Otherwise, the keyboard input remains in the default language.

The IME icon appears in the Windows system tray and indicates the language you are currently using. For example, if you are using English, the IME icon in the system tray displays **EN**. If you are using French, the IME icon in the system tray displays **FR**.

Procedure

1. Click the IME icon in the Windows system tray.

   The system displays a menu with the languages installed on your PC.
2. Select the language you want to use.
3. Type the native name in .

Editing an endpoint

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Endpoint list, select the endpoint you want to edit.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields in the **Edit Endpoint** page.
8. Click **Commit** to save the changes.

Related topics:

[Endpoint / Template field descriptions](#) on page 653

Viewing an endpoint

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the list of endpoints, select the endpoint you want to view.
6. Click **View** to view the attributes of the endpoint you have chosen.

   ✱ **Note:**

   You cannot edit the fields in the View Endpoint page. To go to the Edit Endpoint page, click **Edit**.

Related topics:

[Endpoint / Template field descriptions](#) on page 653

Deleting an endpoint

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Endpoint list, select the endpoints you want to delete.
6. Click **Delete**.

The system displays a confirmation message alerting you to a user associated with the endpoint. The system highlights these user-associated endpoints in yellow color.

> **Note:**
>
> You cannot delete an endpoint associated with a user through endpoint management. You can delete the user associated endpoints only through User Profile Management.

Editing endpoint extensions

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Endpoint list, select the endpoint for which you want to edit the extension.
6. Click **More Actions** > **Edit Endpoint Extension**.
7. Complete the **Edit Endpoint Extension** page and click **Commit** to save the new extension.

   > **Note:**
   >
   > You can use the **Edit Endpoint Extension** option to change the endpoint extension. You can also edit the **Message Lamp Ext** and **Emergency Location Ext** fields through **Edit Endpoint Extension**. Use the **Edit** option to modify the other attributes.

Related topics:

Edit Endpoint Extension field descriptions on page 672

Bulk adding endpoints

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Bulk Add Endpoints**.
6. Complete the **Bulk Add Endpoint** page and click **Commit** to bulk add the endpoints.

   The **Endpoint Name Prefix** field gives the common prefix which appears for all the endpoints you bulk add. You can enter any prefix name of your choice in this field.

   > **Note:**
   >
   > In the **Enter Extensions** field you can enter the extensions which you want to use. You must enter the extensions in serial order and also check for the availability of an extension before you use it.

Related topics:

Bulk Add Endpoint field descriptions on page 673

Bulk editing endpoints

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Endpoint list select the endpoints you want to bulk edit.

6. Click **More Actions** > **Bulk Edit Endpoints**.
7. Complete the **Bulk Edit Endpoint** page and click **Commit** to bulk edit the endpoints.

   The **Endpoint Name Prefix** field gives the common prefix that appears for all the endpoints you bulk add or edit. You can enter any prefix name of your choice in this field.

Related topics:

Bulk Edit Endpoint field descriptions on page 674

Endpoint List

Endpoint List displays all the endpoints under the Communication Managers you select. You can perform an advanced search on the endpoint list using the search criteria. You can also apply filters and sort each of the columns in the Endpoint List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Name	Specifies the name of the endpoint.
Extension	Specifies the extension of the endpoint.
Port	Specifies the port of the endpoint.
Set Type	Specifies the set type of the endpoint.
COS	Specifies the COS for the endpoint.
COR	Specifies the COR for the endpoint.
User	If an endpoint is associated with a user, the system displays the name of the user in this column.
System	Specifies the Communication Manager of the endpoint.

Filtering endpoints

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **Filter: Enable** in the Endpoint List.
6. Filter the endpoints according to one or multiple columns.
7. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

   > **Note:**
   >
   > The table displays only those endpoints that match the filter criteria.

Using Advanced Search

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **Advanced Search** in the Endpoint list .
6. In the Criteria section, do the following:

   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter the search value in the third field.

If you want to add a search condition, click the plus sign (**+**) and repeat the sub steps listed in step 5.

If you want to delete a search condition, click the minus sign (**-**) . This button is available if there is more than one search condition.

Add station Template

Endpoint / Template field descriptions

You can use these fields to perform endpoint / template tasks. This page has the exclusive fields that occur for endpoints and templates apart from the **General options**, **Feature Options**, **Site Data**, **Data Module/Analog Adjunct**, **Abbreviated Call Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.

Field description for Endpoints

Name	Description
System	Specifies the Communication Manager that the endpoint is assigned to.
Template	Specifies all the templates that correspond to the set type of the endpoint.
Set Type	Specifies the set type or the model number of the endpoint.
Name	Specifies the name associated with an endpoint. The name you enter displays on called telephones that have display capabilities. Some messaging applications, such as Communication Manager Messaging recommend that you enter the user's name (last name first) and their extension to identify the telephone. The name entered is also used for the integrated directory.

Field description for Templates

Name	Description
Set Type	Specifies the set type or the model of the endpoint template.

Template Name	Specifies the name of the endpoint template. You can enter the name of your choice in this field.

Extension

The extension for this station.

For a virtual extension, a valid physical extension or a blank can be entered. Blank allows an incoming call to the virtual extension to be redirected to the virtual extension “busy” or “all” coverage path.

Port

The port assigned to the station.

Valid Entry	Usage
01 to 64	First and second numbers are the cabinet number
A to E	Third character is the carrier
01 to 20	Fourth and fifth characters are the slot number
01 to 32	Sixth and seventh characters are the circuit number
x or X	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions.
IP	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have an IP set. This is automatically entered for certain IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.
xxxVmpp	Specifies the media gateway. • xxx is the gateway number, which is in the range 001 to 250. • m is the module number, which is in the range 1 to 9. • pp is the port number, which is in the range 01 to 32.

General Options

This section lets you set the general fields for a station.

COS

The Class of Service (COS) number used to select allowed features.

Continue on Error

Provides the option that during implementing parameter changes, if the system encounters an error, whether the system should continue or abort the implementation.

COR

Class of Restriction (COR) number with the desired restriction.

Coverage Path 1 or Coverage Path 2

The coverage-path number or time-of-day table number assigned to the station.

Note:

If Modified Misoperation is active, a Coverage Path must be assigned to all stations on Communication Manager.

TN

Valid Entry	Usage
1 to 100	The Tenant Partition number.

Security Code

The security code required by users for specific system features and functions, including the following: Personal Station Access, Redirection of Calls Coverage Off-Net, Leave Word Calling, Extended Call Forwarding, Station Lock, Message Retrieval, Terminal Self-Administration, and Demand Printing. The required security code length is administered system-wide.

Emergency Location Ext

The Emergency Location Extension for this station. This extension identifies the street address or nearby location when an emergency call is made. Defaults to the telephone’s extension. Accepts up to thirteen digits.

Note:

On the ARS Digit Analysis Table in Communication Manager, 911 must be administered to be call type emer or alrt for the E911 Emergency feature to work properly.

Message Lamp Ext

The extension of the station tracked with the message waiting lamp.

Lock Messages

Controls access to voice messages by other users.

Valid Entry	Usage
y	Restricts other users from reading or canceling the voice messages, or retrieving messages using Voice Message Retrieval.

Valid Entry	Usage
n	Allows other users to read, cancel, or retrieve messages.

Feature Options

This section lets you set features unique to a particular voice terminal type.

Location

This field appears only when the **Multiple Locations** field is set to y and the **Type** field is set to H.323 or SIP station types.

Valid entry	Usage
1 to 250	(Depending on your server configuration, see *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.) Assigns the location number to a particular station. Allows IP telephones and softphones connected through a VPN to be associated with the branch an employee is assigned to. This field is one way to associate a location with a station. For the other ways and for a list of features that use location, see the Location sections in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.
blank	Indicates that the existing location algorithm applies. By default, the value is blank.

DTMF Over IP

Specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling. Available only if **Group Type** is sip.

Valid Entry	Usage
in-band	All G711 and G729 calls pass DTMF in-band. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G.723 is sent out-of-band.
in-band-g711	Only G711 calls pass DTMF in-band.
out-of-band	All IP calls pass DTMF out-of-band. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This value is not supported for SIP signaling. This is the default for newly added H.323 signaling groups.
rtp-payload	This method is specified by RFC 2833. By default, RFC 2833 is the default value for newly added SIP signaling groups. Support for SIP trunks requires the default entry of rtp-payload.

Active Station Ringing

Defines how calls ring to the telephone when it is off-hook without affecting how calls ring at this telephone when the telephone is on-hook.

Valid Entry	Usage
continuous	All calls to this telephone ring continuously.
single	Calls to this telephone receive one ring cycle and then ring silently.
if-busy-single	Calls to this telephone ring continuously when the telephone is off-hook and idle. Calls to this telephone receive one ring cycle and then ring silently when the telephone is off-hook and active.
silent	All calls to this station ring silently.

Auto Answer

In EAS environments, the auto answer setting for the Agent LoginID can override a station's setting when an agent logs in.

Valid Entry	Usage
all	All ACD and non-ACD calls terminated to an idle station cut through immediately. Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when the **Allow Ringer-off with Auto-Answer** is enabled for the system.
acd	Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls terminated to a station ring audibly. For analog stations, the station is off-hook and idle, only the ACD split/ skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the station is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone.
none	All calls terminated to this station receive an audible ringing treatment.
icom	Allows a telephone user to answer an intercom call from the same intercom group without pressing the **intercom** button.

MWI Served User Type

Controls the auditing or interrogation of a served user's message waiting indicator (MWI).

Valid Entries	Usage
fp-mwi	The station is a served user of an fp-mwi message center.
qsig-mwi	The station is a served user of a qsig-mwi message center.
blank	The served user's MWI is not audited or if the user is not a served user of either an fp-mwi or qsig-mwi message center.

Coverage After Forwarding

Governs whether an unanswered forwarded call is provided coverage treatment.

Valid Entry	Usage
y	Coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters.

Valid Entry	Usage
n	No coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters.
s(ystem)	Administered system-wide coverage parameters determine treatment.

Per Station CPN - Send Calling Number

Determines Calling Party Number (CPN) information sent on outgoing calls from this station.

Valid Entries	Usage
y	All outgoing calls from the station deliver the CPN information as “Presentation Allowed.”
n	No CPN information is sent for the call.
r	Outgoing non-DCS network calls from the station delivers the Calling Party Number information as “Presentation Restricted.”
blank	The sending of CPN information for calls is controlled by administration on the outgoing trunk group the calls are carried on.

Display Language

Valid Entry	Usage
english french italian spanish user-defined	The language that displays on stations. Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.).
unicode	Displays English messages in a 24-hour format . If no Unicode file is installed, displays messages in English by default. **Note:** Unicode display is only available for Unicode-supported telephones. Currently, 4610SW, 4620SW, 4621SW, 4622SW, 16xx, 96xx, 96x1, and 9600-series telephones (Avaya one-X Deskphone Edition SIP R2 or later) support Unicode display. Unicode is also an option for DP1020 (aka 2420J) and SP1020 (Toshiba SIP Phone) telephones when enabled for the system.

Personalized Ringing Pattern

Defines the personalized ringing pattern for the station. Personalized Ringing allows users of some telephones to have one of 8 ringing patterns for incoming calls. For virtual stations, this field dictates the ringing pattern on its mapped-to physical telephone.

L = 530 Hz, M = 750 Hz, and H = 1060 Hz

Valid Entries	Usage
1	MMM (standard ringing)

Valid Entries	Usage
2	HHH
3	LLL
4	LHH
5	HHL
6	HLL
7	HLH
8	LHL

Hunt-to Station

The extension the system should hunt to for this telephone when the telephone is busy. A station hunting chain can be created by assigning a hunt-to station to a series of telephones.

Remote Softphone Emergency Calls

TellsCommunication Manager how to handle emergency calls from the IP telephone.

⚠ **Caution:**

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. Please be advised that an Avaya IP endpoint cannot dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. Do not use an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones.

Available only if the station is an IP Softphone or a remote office station.

Valid Entry	Usage
as-on-local	If the emergency location extension that corresponds to this station's IP address is not administered (left blank), the value as-on-local sends the station emergency location extension to the Public Safety Answering Point (PSAP). If the administrator populates the IP address mapping with emergency numbers, the value as-on-local functions as follows: • If the station emergency location extension is the same as the IP address mapping emergency location extension, the value as-on-local sends the station's own extension to the Public Safety Answering Point (PSAP). • If the station emergency location extension is different from the IP address mapping emergency location extension, the value as-on-

Valid Entry	Usage
	local sends the IP address mapping extension to the Public Safety Answering Point (PSAP).
block	Prevents the completion of emergency calls. Use this entry for users who move around but always have a circuit-switched telephone nearby, and for users who are farther away from the server than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP Telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.
cesid	Allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. The end user enters the emergency information into the IP Softphone. Use this entry for IP Softphones with road warrior service that are near enough to the server that an emergency call routed over the it's trunk reaches the PSAP that covers the server or switch. If the server uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the server uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP Softphone location, based on advice from the local emergency response personnel.
option	Allows the user to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported. This entry is used for extensions that can be swapped back and forth between IP Softphones and a telephone with a fixed location. The user chooses between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects the extension.

Service Link Mode

Determines the duration of the service link connection. The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and a server running Avaya Communication Manager that terminates the H.320 protocol. When the user receives or makes a call during a multimedia or IP Softphone or IP Telephone session, a "service link" is established.

Valid Entry	Usage
as-needed	Used for most multimedia, IP Softphone, or IP Telephone users. Setting the Service Link Mode to as-needed leaves the service link connected for 10 seconds after the user ends a call so that they can immediately place or take another call. After 10 seconds the link is dropped and a new link would have to be established to place or take another call.
permanent	Used for busy call center agents and other users who are constantly placing or receiving multimedia, IP Softphone, or IP Telephone calls. In permanent mode, the service link stays up for the duration of the multimedia, IP Softphone, or IP Telephone application session.

Loss Group

Valid Entry	Usage
1 to 17	Determines which administered two-party row in the loss plan applies to each station. Does not appear for stations that do not use loss — such as x-mobile stations and MASI terminals.

Speakerphone

Controls the behavior of speakerphones.

Valid Entry	Usage
1-way	Indicates that the speakerphone listen-only.
2-way	Indicates that the speakerphone is both talk and listen.
grp-listen	Group Listen allows a telephone user to talk and listen to another party with the handset or headset while the telephone's two-way speakerphone is in the listen-only mode. Others in the room can listen, but cannot speak to the other party through the speakerphone. The person talking on the handset acts as the spokesperson for the group. Group Listen provides reduced background noise and improves clarity during a conference call when a group needs to discuss what is being communicated to another party. Available only with 6400-series and 2420/2410 telephones.
none	Not administered for a speakerphone.

LWC Reception

Indicates where Leave Word Calling (LWC) messages are stored.

Valid Entry	Usage
audix	LWC messages are stored on the voice messaging system.
none	LWC messages are not be stored.
spe	LWC messages are stored in the system or on the switch processor element (spe).

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.

Time of Day Lock Table

Valid Entry	Usage
1 to 5	Assigns the station to a Time of Day (TOD) Lock/Unlock table. The assigned table must be administered and active.
blank	Indicates no TOD Lock/Unlock feature is active. This is the default.

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.

Media Complex Ext

When used with Multi-media Call Handling, indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to place either a voice or a data call, and voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.

Valid Entry	Usage
A valid BRI data extension	For MMCH, enter the extension of the data module that is part of this multimedia complex.
H.323 station extension	For 4600 series IP Telephones, enter the corresponding H.323 station. For IP Softphone, enter the corresponding H.323 station. If you enter a

Valid Entry	Usage
	value in this field, you can register this station for either a road-warrior or telecommuter/Avaya IP Agent application.
blank	Leave this field blank for single-connect IP applications.

AUDIX Name

The voice messaging system associated with the station. Must contain a user-defined adjunct name that was previously administered.

Call Appearance Display Format

Specifies the display format for the station. Bridged call appearances are not affected by this field. This field is available only on telephones that support downloadable call appearance buttons, such as the 2420 and 4620 telephones.

Note:

This field sets the administered display value only for an individual station.

Valid Entry	Usage
loc-param-default	The system uses the administered system-wide default value. This is the default.
inter-location	The system displays the complete extension on downloadable call appearance buttons.
intra-location	The system displays a shortened or abbreviated version of the extension on downloadable call appearance buttons.

IP Phone Group ID

Available only for H.323 station types.

Valid Entry	Usage
0 to 999 blank	The Group ID number for this station.

Always Use

Enables or disables the following emergency call handling settings:

- A softphone can register no matter what emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the administered **Emergency Location Extension** is used. The softphone's user-entered settings are ignored.
- If an IP telephone dials 911, the administered **Emergency Location Extension** is used.
- If a call center agent dials 911, the physical station extension is displayed, overriding the administered **LoginID for ISDN Display** .

Does not apply to SCCAN wireless telephones, or to extensions administered as type h.323.

Audible Message Waiting

Enables or disables an audible message waiting tone indicating the user has a waiting message consisting of a stutter dial tone when the user goes off-hook.

This field does *not* control the Message Waiting lamp.

Available only if **Audible Message Waiting** is enabled for the system.

Auto Select Any Idle Appearance

Enables or disables automatic selection of any idle appearance for transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Communication Manager selects the first idle appearance.

Bridged Call Alerting

Controls how the user is alerted to incoming calls on a bridged appearance.

Valid Entry	Usage
y	The bridged appearance rings when a call arrives at the primary telephone.
n	The bridged appearance flashes but does not ring when a call arrives at the primary telephone. This is the default. If disabled and **Per Button Ring Control** is also disabled, audible ringing is suppressed for incoming calls on bridged appearances of another telephone's primary extension.

Bridged Idle Line Preference

Specifies whether the selected line for incoming bridged calls is always an idle line.

Valid Entry	Usage
y	The user connects to an idle call appearance instead of the ringing call.
n	The user connects to the ringing call appearance.

CDR Privacy

Enables or disables Call Privacy for each station. Allows digits in the called number field of an outgoing call record to be blanked on a per-station basis. The number of blocked digits is administered system-wide as CDR parameters.

Conf/Trans On Primary Appearance

Enables or disables the forced use of a primary appearance when the held call to be conferenced or transferred is a bridge. This is regardless of the administered value for **Auto Select Any Idle Appearance** .

Coverage Msg Retrieval

Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.

IP Video

Enables or disables IP video capability for this signaling group. Available only if the signaling group type h.323 and sip.

Data Restriction

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

Direct IP-IP Audio Connections

Allows or denies direct audio connections between IP endpoints that saves on bandwidth resources and improves sound quality of voice over IP transmissions.

Display Client Redirection

Enables or disables the display of redirection information for a call originating from a station with Client Room Class of Service and terminating to this station. When disabled, only the client name and extension or room display. Available only if Hospitality is enabled for the system.

> **Note:**
>
> This field must be enabled for stations administered for any type of voice messaging that needs display information.

Select Last Used Appearance

Valid Entry	Usage
y	Indicates a station's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. The line selection on an on-hook station only moves from the last used line button to a line button with an audibly alerting call. If there are no alerting calls, the line selection remains on the button last used for a call.
n	The line selection on an on-hook station with no alerting calls can be moved to a different line button that might be serving a different extension.

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.

Valid Entry	Usage
n	Prevents this station from receiving incoming trunk calls when in survivable mode.

H.320 Conversion

Enables or disables the conversion of H.320 compliant calls made to this telephone to voice-only. Because the system can handle only a limited number of conversion calls, the number of telephones with H.320 conversion should be limited.

Idle Appearance Preference

Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.

Valid Entry	Usage
y	The user connects to an idle call appearance instead of the ringing call.
n	The Alerting Appearance Preference is set and the user connects to the ringing call appearance.

IP Audio Hairpinning

Enables or disables hairpinning for H.323 or SIP trunk groups. H.323 and SES-enabled endpoints are connected through the IP circuit pack without going through the time division multiplexing (TDM) bus. Available only if **Group Type** is h.323 or sip.

IP Softphone

Indicates whether or not this extension is either a PC-based multifunction station or part of a telecommuter complex with a call-back audio connection.

Available only for DCP station types and IP Telephones.

LWC Activation

Activates or deactivates the Leave Word Calling (LWC) feature. LWC allows internal telephone users on this extension to leave short pre-programmed messages for other internal users.

LWC should be used if:

- The system has hospitality and the guest-room telephones require LWC messages indicating that wakeup calls failed
- LWC messages are stored in a voice-messaging system

LWC Log External Calls

Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls provided information on the caller identification is available. Each record consists of the latest call attempt date and time.

Multimedia Early Answer

Enables or disables multimedia early answer on a station-by-station basis.

The station should be enabled for this feature if the station receives coverage calls for multimedia complexes, but is not multimedia-capable. This ensures that calls are converted and the talk path is established before ringing at this station.

Mute Button Enabled

Enables or disables the mute button on the station.

Per Button Ring Control

Enables or disables per button ring control by the station user.

Valid Entries	Usage
y	Allows users to select ring behavior individually for each call-appr, brdg-appr, or abrdg-appr on the station and to enable Automatic Abbreviated and Delayed ring transition for each call-appr on the station. Prevents the system from automatically moving the line selection to a silently alerting call unless that call was audibly ringing earlier.
n	Calls on **call-appr** buttons always ring the station and calls on **brdg-appr** or **abrdg-appr** buttons always ring or not ring based on the **Bridged Call Alerting** value. Allows the system to move line selection to a silently alerting call if there is no call audibly ringing the station.

Precedence Call Waiting

Activates or deactivates Precedence Call Waiting for this station.

Redirect Notification

Enables or disables redirection notification that gives a half ring at this telephone when calls to this extension are redirected through Call Forwarding or Call Coverage. Must be enabled if LWC messages are stored on a voice-messaging system.

Restrict Last Appearance

Valid Entries	Usage
y	Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only.
n	Last idle call appearance is used for incoming priority calls and outgoing call originations.

EMU Login Allowed

Enables or disables using the station as a visited station by an Enterprise Mobility User (EMU).

Bridged Appearance Origination Restriction

Restricts or allows call origination on the bridged appearance.

Valid Entry	Usage
y	Call origination on the bridged appearance is restricted.

Valid Entry	Usage
n	Call origination ion the bridged appearance is allowed. This is normal behavior, and is the default.

Voice Mail Number

The complete Voice Mail Dial Up number. Accepts up to 17 digits.

Site Data

This section lets you set information about the Room, Floor, Jack, Cable, Mounting, and Building.

Room

Valid Entry	Usage
Telephone location	Identifies the telephone location. Accepts up to 10 characters.
Guest room number	Identifies the guest room number if this station is one of several to be assigned a guest room and the **Display Room Information in Call Display** is enabled for the system. Accepts up to five digits.

Floor

A valid floor location.

Jack

Alpha-numeric identification of the jack used for this station.

Cable

Identifies the cable that connects the telephone jack to the system.

Mounting

Indicates whether the station mounting is d(esk) or w(all).

Building

A valid building location.

Set Color

Indicates the set color. Valid entries include the following colors: beige, black, blue, brown, burg (burgundy), gray, green, ivory, orng (orange), red, teak, wal (walnut), white, and yel (yellow).

You can change the list of allowed set colors by using the Valid Set Color fields on the site-data screen.

Cord Length

The length of the cord attached to the receiver. This is a free-form entry, and can be in any measurement units.

Headset

Indicates whether or not the telephone has a headset.

Speaker

Indicates whether or not the station is equipped with a speaker.

Abbreviated Call Dialing

This section lets you create abbreviated dialing lists for a specific station, and provide lists of stored numbers that can be accessed to place local, long-distance, and international calls; allows you to activate features or access remote computer equipment and select enhanced, personal, system or group lists.

Abbreviated Dialing List 1, List 2, List 3

Assigns up to three abbreviated dialing lists to each telephone.

Valid Entry	Usage
enhanced	Allows the telephone user to access the enhanced system abbreviated dialing list.
group	Allows the telephone user to access the specified group abbreviated dialing list. Requires administration of a group number.
personal	Allows the telephone user to access and program their personal abbreviated dialing list. Requires administration of a personal list number.
system	Allows the telephone user to access the system abbreviated dialing list.

Personal List

Establishes a personal dialing list for telephone or data module users. The personal list must first be assigned to the telephone by the System Administrator before the telephone user can add entries in the list. Users access the lists in order to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `change abbreviated-dialing personal`

Abbreviated Dialing Enhanced List

Establishes system-wide or personal lists for speed dialing.

The Enhanced Abbreviated Dialing List can be accessed by users to place local, long-distance, and international calls; to activate or deactivate features; or to access remote computer equipment.

Note:

Dialing must be enabled in the license file before the Enhanced List can be programmed.

Example command: `display abbreviated-dialing enhanced`

Group List

Implements the Abbreviated Dialing Group List. The System Administrator controls the Group Lists. Up to 100 numbers can be entered for every group list. Users can access this list to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `change abbreviated-dialing group`

Enhanced Call Fwd

This section allows you to specify the destination extension for the different types of call forwards.

Forwarded Destination

A destination extension for both internal and external calls for each of the three types of enhanced call forwarding (Unconditional, Busy, and No Reply). Accepts up to 18 digits. The first digit can be an asterisk *.

Requires administration to indicate whether the specific destination is active (enabled) or inactive (disabled).

SAC/CF Override

Allows the user of a station with a **Team** button administered, who is monitoring another station, to directly reach the monitored station by pushing the **Team** button. This overrides any currently active rerouting, such as Send All Calls and Call Forwarding, on the monitored station.

Valid Entries	Usage
Ask	The system asks if the user wants to follow the rerouting or override it. When the user has the option to decide whether rerouting should take place or not, a message is sent to the station that displays the active rerouting and the number of the forwarded to station.
No	Cannot override rerouting. The station does not have the ability to override the rerouting of a monitored station.
Yes	Can override rerouting. The station has the ability to override the rerouting the monitored station has set, as long as one incoming call appearance is free.

Button Assignment

This section lets you assign features to the buttons on a phone. You can assign the main buttons for your station by choosing an option from the list down box for each button.

Group Membership

This section describes the different groups that an extension can be a member of. You should select the station you want to group and then choose the group from the drop-down box, before clicking **Commit**.

Understanding groups

Your voice system uses groups for a number of different purposes. This topic describes the different groups that an extension can be a member of. However, your voice system may include other types of groups as well (for example, trunk groups). For information on those groups, see the Administrator’s Guide to Communication Manager Software.

Your voice system may have any of the following types of groups set up:

Type	Description
group page	Group page is a feature that allows you to make an announcement to a pre-programmed group of phone users. The announcement is heard through the speakerphone built into some sets. Users will hear the announcement if their set is idle. Users cannot respond to the announcement.
coverage answer group	A coverage answer group lets up to 8 phones ring simultaneously when a call is redirected to the group.
coverage path	A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call. For more information on coverage paths, see "Creating Coverage Paths" in the Administrator’s Guide to Communication Manager Software.
hunt group	A hunt group is a group of extensions that receive calls according to the call distribution method you choose. When a call is made to a certain phone number, the system connects the call to an extension in the group. Use hunt groups when you want more than one person to be able to answer calls to the same number. For more information on hunt groups, see "Managing Hunt Groups" in the Administrator’s Guide to Communication Manager Software.

intercom group	An intercom group is a group of extensions that can call each other using the intercom feature. With the intercom feature, you can allow one user to call another user in a predefined group just by pressing a couple of buttons. For more information on intercom groups, see "Using Phones as Intercoms" in the Administrator's Guide to Communication Manager Software.
pickup group	A pickup group is a group of extensions in which one person may pick up another person's calls. For more information on pickup groups, see "Adding Call Pickup" in the Administrator's Guide to Communication Manager Software.
terminating extension group	A Terminating Extension Group (TEG) allows an incoming call to ring as many as 4 phones at one time. Any user in the group can answer the call. For more information on terminating extension groups, see "Assigning a Terminating Extension Group" in the Administrator's Guide to Communication Manager Software.

Edit Endpoint Extension field descriptions

Use this page to change the extension of an endpoint.

Field	Description
System	Specifies the list of Communication Managers. Select one of the options.
Extension	Extension of the device you want to change.
New Extension	New extension you want to provide for the device.
Emergency location extension	Existing emergency location extension of your device.
New emergency location extension	New existing emergency location extension you want to provide.

Field	Description
Message lamp extension	Existing message lamp extension of your device.
New message lamp extension	New message lamp extension you want to provide.

Button	Description
Commit	Saves the new extension.
Schedule	Saves the extension at the scheduled time.
Reset	Clears all the entries.
Cancel	Takes you back to the previous page.

Bulk Add Endpoint field descriptions

Field	Description
Template	The template you choose for the endpoints.
Station name prefix	Specifies the prefix name that appears for each of the endpoints you add. You can enter a prefix name of your choice in this field.
System	Specifies the list of the Communication Managers.
Available extensions	The list of extensions that are available.
Enter extensions	The extensions that you want to use. You can enter your preferred extensions in this field.

Button	Description
Commit	Bulk adds the endpoints.
Schedule	Bulk adds the station at the scheduled time.
Clear	Undoes all the entries.
Cancel	Takes you to the previous page.

Bulk Edit Endpoint field descriptions

Name	Description
Template	Specifies the endpoint template. You can choose the template which you want to bulk edit.
Station Name Prefix	Specifies the prefix name which appears before all the endpoints that you bulk edit. You can enter a prefix name of your choice.

Button	Description
Commit	Bulk edits the endpoints.
Schedule	Bulk edits the endpoints at the specified time.
Clear	Undoes the entries.
Cancel	Takes you to the previous page.

Changing endpoint parameters globally

You can use the Global Change Endpoint capability to specify several aspects of a task to modify endpoints on one or more Communication Manager elements.

You can use this capability to conduct a global search-and-filter operation on endpoints across multiple PBXs, and select endpoint properties to which you want to apply a common value across the filtered selection. For example, you can find all buttons with a specific assign and change the parameters for all those buttons, locate new buttons without overwrite, and change the set type of many endpoints simultaneously as you move from digital to IP or SIP.

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select the endpoints for which you want to change the parameters from the Endpoints List.
4. Click **More Actions** > **Global Change Endpoint**.

5. Enter the filter criteria on the **Global Endpoint Search and Replace** page.
6. Click **Search**. The system displays endpoints in the Endpoint List based on the filter criteria.

   By default, the check boxes for all the endpoints are selected in this list. You can choose to clear the selection for the endpoints whose parameters you do not wish to change.
7. Click **Proceed to change parameters**.
8. On the Endpoint Changes page, enter the values in the parameter fields that you want to change.
9. Click **Commit** to change the endpoints parameters or do one of the following:
   - Click **Schedule** to change the endpoints parameters at a specified time.
   - Click **Cancel** to cancel the operation.

Changing to classic view in Endpoints

The Manage Endpoints Web interface supports two types of views, classic view and enhanced view. Enhanced view is the default setting where you can execute endpoint-related activities on the Web interface. In the classic view, the system directs you to Element Cut Through screen for executing endpoint-related activities. To change to classic view, use the **Switch to Classic View** link. To return to default view, you need to click the **Switch to Enhanced View** link

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Click the **Switch to Classic View** link on the upper-right of the interface.

Viewing endpoint status

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.

2. Click **Endpoints** > **Manage Endpoints** in the left navigation page.
3. From the Endpoint List, select the endpoints whose status you want to view.
4. Click **Maintenance** > **Status**.

Result

The system displays the status of the selected endpoint on the Element Cut Through screen.

Related topics:

Endpoint / Template field descriptions on page 653

Busy out endpoints

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation page.
3. Select the endpoints you want to busy out from the Endpoint List.

   ! **Important:**

   This maintenance operation is service affecting.
4. Click **Maintenance** > **Busyout Endpoint**.
5. On the Busyout Endpoint Confirmation page, click **Now** to busy out the endpoints or do one of the following:
   - Click **Schedule** to perform the busy out at a specified time.
   - Click **Cancel** to cancel the busy out.

Result

The system displays the result of the busy out operation on the **Busyout Endpoint Report** page.

Related topics:

Endpoint / Template field descriptions on page 653

Releasing endpoints

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation page.
3. Select the endpoints you want to release from the Endpoint List.

   ❗ **Important:**

   This maintenance operation is service affecting.
4. Click **Maintenance** > **Release Endpoint**.
5. On the **Release Endpoint Confirmation** page, click **Now** to release the endpoints or do one of the following:
   - Click **Schedule** to perform the release at a specified time.
   - Click **Cancel** to cancel the release.

Result

The system displays the result of the release operation on the **Release Endpoint Report** page.

Related topics:

Endpoint / Template field descriptions on page 653

Testing endpoints

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Endpoints** > **Manage Endpoints** in the left navigation pane.
3. Select the endpoints you want to test from the Endpoint List.

   ❗ **Important:**

   This maintenance operation is service affecting.

4. Click **Maintenance** > **Test Endpoint**.
5. On the Test Endpoint Confirmation page, click **Now** to test the endpoints or do one of the following:
    - Click **Schedule** to test the endpoints at a specified time.
    - Click **Cancel** to cancel the test operation.

Result

The system displays the **Test Endpoint Report** page, where you can view the test result and error code of the endpoint. You can click the **Error Code Description** link to view the error details.

Related topics:

Endpoint / Template field descriptions on page 653

Error codes on page 678

Error codes

Following table gives the common error codes for Busyout, Release, Test, and Reset Commands lists. This table also has the common error codes associated with abort and fail results for busyout, release, test, and reset commands. In addition to these, many maintenance objects have other unique error codes.

Error Code	Command Result	Description/Recommendation
	ABORT	System resources are unavailable to run command. Try the command again at 1-minute intervals up to 5 times.
0	ABORT	Internal system error. Retry the command at 1-minute intervals up to 5 times.
1005	ABORT	A DS1 interface circuit pack could not be reset because it is currently supplying the on-line synchronization reference. Use set sync to designate a new DS1 interface circuit pack as the on-line reference, then try the reset again.
1010	ABORT	Attempt was made to busyout an object that was already busied out.
1011	ABORT	Attempt was made to release an object that was not first busied out.
1015	ABORT	A reset of this circuit pack requires that every maintenance object on it be in the out-of-service state. Use busyout board

		to place every object on the circuit pack in the out-of-service state, and try the reset again.
1026	ABORT	The specified TDM bus cannot be busied out because the control channel or system tones are being carried on it. Use set tdm PC to switch the control channel and system tones to the other TDM bus.
2012 2500	ABORT	Internal system error.
2100	ABORT	System resources to run this command were unavailable. Try the command again at 1-minute intervals up to 5 times.
62524 62525 62526	ABORT	Maintenance is currently active on the maximum number of maintenance objects that the system can support. A common cause is that the system contains a large number of administered stations or trunks with installed circuit packs that are not physically connected. Resolve as many alarms as possible on the station and trunk MOs, or busyout these MOs to prevent maintenance activity on them. Then try the command again.
	NO BOARD	The circuit pack is not physically installed.
2100	EXTRA BD	This result can appear for: S8700 Maintenance/Test, Announcement circuit packs S8700 MC Call Classifier, Tone Detector, Speech Synthesis circuit packs Each of these circuit packs has restrictions on how many can be installed in the system or in a port network, depending on system configuration. Remove any extra circuit packs.
1	FAIL	For reset commands, the circuit pack was not successfully halted.
2	FAIL	For reset commands, the circuit pack was not successfully restarted after being halted. For both results replace the circuit pack.
	FAIL	See the applicable maintenance object (from the Maintenance Name field) in Maintenance Alarms Reference, 03-300190.
	PASS	The requested action successfully completed. If the command was a reset, the circuit pack is now running and should be tested.

Chapter 25: Templates

Template management

A template is a file that contains stored settings. You can use templates to streamline the process of performing various routine activities. Templates save the data that you enter so that you can perform similar activities later without re-entering the same data. With System Manager, you can create, store, and use templates to simplify tasks like adding, editing, and viewing endpoints or subscribers. In System Manager, there are several default templates and you can create your own templates as well.

Templates exist in two categories, default templates and user-defined templates. The default templates exist on the system and you cannot edit or remove them. You can, however, modify or remove user-defined templates any time.

Template versioning

Template versioning

You can version endpoint templates with Communication Manager 5.0, Communication Manager 5.1, Communication Manager 5.2, and Communication Manager 6.0. You can associate a template with a specific version of a Communication Manager or an adopting product through template versioning. You can use the **Template Version** field under endpoint templates to accommodate endpoint template versioning.

You can also use template versioning for subscriber templates using the following versions: Aura Messaging 6.0, MM 5.0, MM 5.1, MM 5.2, MM 6.0, CMM 5.2, and CMM 6.0.

Adding endpoint templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Templates** > **Endpoint** in the left navigation pane.
3. Click **New**.

4. Click **Set type**.
5. Enter a name in the **Template Name** field.
6. Complete the mandatory fields under the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.
7. Click **Commit**.

Related topics:

Endpoint / Template field descriptions on page 653

Editing endpoint templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Endpoint** in the left navigation pane.
3. Select the template you want to edit from the template list.
4. Click **Edit** or click **View** > **Edit**.
5. Complete the **Edit Endpoint Template** page.
6. Click **Commit** to save the changes.

Related topics:

Endpoint / Template field descriptions on page 653

Viewing endpoint templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Endpoint** in the left navigation pane.
3. Select the template you want to view.
4. Click **View**.

You can view the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Call Dialing**, **Enhanced Call Fwd**, and **Button Assignment** sections on the View Endpoint Template page.

Related topics:
Endpoint / Template field descriptions on page 653

Deleting endpoint templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Endpoint** in the left navigation pane.
3. Select the endpoint templates you want to delete from the endpoint template list.
4. Click **Delete**.

   Note:
   You cannot delete any of the default templates.

Duplicating endpoint templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Endpoint** in the left navigation pane.
3. Select the template you want to copy from the endpoint template list.
4. Click **Duplicate**.
5. Enter the name of the new template in the **New Template Name** field.
6. Choose the appropriate set type from the **Set Type** field.
7. Complete the **Duplicate Endpoint Template** page and click **Commit**.

Related topics:
Endpoint / Template field descriptions on page 653

Distribution of templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Endpoint** on the left navigation pane.
3. Select an endpoint template from the endpoint template list.
4. Click **More Actions** > **Distribute**.
5. Select the Communication Manager systems to which you want to distribute the template you have chosen.
6. Click **Commit** to distribute the template value.
   All the endpoints associated with this template for the selected Communication Manager systems now have the same field values as that in the template.

Viewing associated endpoints

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Endpoint** in the left navigation pane.
3. Select an endpoint template from the endpoint templates list.
4. Click **More Actions** > **View Associated Endpoints**.
   You can view the endpoints in the System Manager database that are associated with the endpoint template you have chosen on the Associated Endpoints page.

Adding subscriber templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Messaging** in the left navigation pane.

3. Select a messaging version from the list of supported messaging versions.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions** and **Miscellaneous** sections in the Add Subscriber Template page.
7. Click **Commit**.

   Subscriber templates have different versions based on the software version. The subscriber templates you create have to correspond to the Messaging, MM, or CMM software version. When you select a messaging template, the **Software Version** field in the Add Subscriber Template page displays the appropriate version information.

Related topics:

Subscriber Templates (CMM) field descriptions on page 709

Subscriber Templates (MM) field descriptions on page 712

Editing subscriber templates

About this task

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Messaging** in the left navigation pane.
3. From the supported messaging version list, select a messaging version.
4. Click **Show List**.
5. Select a subscriber template from the Subscriber Template list.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields on the **Edit Subscriber Template** page.
8. Click **Commit** to save the changes.

   Note:

   You cannot edit any of the default subscriber templates.

Related topics:

Subscriber Templates (CMM) field descriptions on page 709
Subscriber Templates (MM) field descriptions on page 712

Viewing subscriber templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Messaging** in the left navigation pane.
3. From the supported messaging versions list, select one of the messaging versions.
4. Click **Show List**.
5. Select a subscriber template from the Subscriber Template list.
6. Click **View** to view the mailbox settings of this subscriber.

   Note:

   You cannot edit any of the fields in the View Subscriber Template page.

Related topics:

Subscriber Templates (CMM) field descriptions on page 709
Subscriber Templates (MM) field descriptions on page 712

Deleting subscriber templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Messaging** in the left navigation pane.
3. From the list of supported messaging versions, select a supported messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select the templates you want to delete.
6. Click **Delete**.

Note:

You cannot delete any default subscriber template.

Duplicating subscriber templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**
2. Click **Messaging** in the left navigation pane.
3. From the list of supported messaging versions, select a messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select the subscriber template you want to copy.
6. Click **Duplicate**.
7. Complete the Duplicate Subscriber Template page and click **Commit**.

Related topics:

Subscriber Templates (CMM) field descriptions on page 709
Subscriber Templates (MM) field descriptions on page 712

Viewing associated subscribers

Procedure

1. On the System Manager console, under **Services**, click **Templates**.
2. Click **Messaging** in the left navigation pane.
3. From the list of supported messaging versions, select a messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select a subscriber template for which you want to view the associated subscribers.
6. Click **More Actions** > **View Associated Subscribers**.

You can view all the associated subscribers in the System Manager database for the template you have chosen in the Associated Subscribers page.

Template list

You can view the template list when you click **Template** under **Services** on the System Manager console. You need to click the **Endpoint** or **Messaging** option to view the endpoint or messaging template list.

You can apply filters and sort each of the columns in the endpoint or messaging template list. When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Name	Name of the template.
Owner	Specifies the name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates this field specifies the name of the user who created the template.
Version	Specifies the version of the template.
Default	Specifies whether the template is default or user-defined.
Last Modified	Specifies the time and date when the endpoint or messaging template was last modified.
Set type (for endpoint templates)	Specifies the set type of the endpoint template.
Type (for messaging templates)	Specifies whether the messaging type is Messaging, MM, or CMM.
Software Version (for messaging templates)	Specifies the type of messaging version of the messaging template.

Filtering templates

Procedure

1. On the System Manager console, under **Services**, click **Templates**.

2. Click either **Endpoint** or **Messaging** for endpoint templates and messaging templates respectively.
3. Select the Communication Manager or supported messaging version, whichever applicable.
4. Click **Show List**.
5. Click **Filter: Enable** in the Template List.
6. Filter the endpoint or subscriber templates according to one or multiple columns.
7. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

   Note:

   The table displays only those endpoint or subscriber templates that match the filter criteria.

Add station Template

Endpoint / Template field descriptions

You can use these fields to perform endpoint / template tasks. This page has the exclusive fields that occur for endpoints and templates apart from the **General options**, **Feature Options**, **Site Data**, **Data Module/Analog Adjunct**, **Abbreviated Call Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.

Field description for Endpoints

Name	Description
System	Specifies the Communication Manager that the endpoint is assigned to.
Template	Specifies all the templates that correspond to the set type of the endpoint.
Set Type	Specifies the set type or the model number of the endpoint.
Name	Specifies the name associated with an endpoint. The name you enter displays on called telephones that have display

	capabilities. Some messaging applications, such as Communication Manager Messaging recommend that you enter the user’s name (last name first) and their extension to identify the telephone. The name entered is also used for the integrated directory.

Field description for Templates

Name	Description
Set Type	Specifies the set type or the model of the endpoint template.
Template Name	Specifies the name of the endpoint template. You can enter the name of your choice in this field.

Extension

The extension for this station.

For a virtual extension, a valid physical extension or a blank can be entered. Blank allows an incoming call to the virtual extension to be redirected to the virtual extension “busy” or “all” coverage path.

Port

The port assigned to the station.

Valid Entry	Usage
01 to 64	First and second numbers are the cabinet number
A to E	Third character is the carrier
01 to 20	Fourth and fifth characters are the slot number
01 to 32	Sixth and seventh characters are the circuit number
x or X	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions.
IP	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the

Valid Entry	Usage
	extension would have an IP set. This is automatically entered for certain IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.
xxxVmpp	Specifies the media gateway. • xxx is the gateway number, which is in the range 001 to 250. • m is the module number, which is in the range 1 to 9. • pp is the port number, which is in the range 01 to 32.

General Options

This section lets you set the general fields for a station.

COS

The Class of Service (COS) number used to select allowed features.

Continue on Error

Provides the option that during implementing parameter changes, if the system encounters an error, whether the system should continue or abort the implementation.

COR

Class of Restriction (COR) number with the desired restriction.

Coverage Path 1 or Coverage Path 2

The coverage-path number or time-of-day table number assigned to the station.

Note:

If Modified Misoperation is active, a Coverage Path must be assigned to all stations on Communication Manager.

TN

Valid Entry	Usage
1 to 100	The Tenant Partition number.

Security Code

The security code required by users for specific system features and functions, including the following: Personal Station Access, Redirection of Calls Coverage Off-Net, Leave Word Calling, Extended Call Forwarding, Station Lock, Message Retrieval, Terminal Self-Administration, and Demand Printing. The required security code length is administered system-wide.

Emergency Location Ext

The Emergency Location Extension for this station. This extension identifies the street address or nearby location when an emergency call is made. Defaults to the telephone’s extension. Accepts up to thirteen digits.

✱ **Note:**

On the ARS Digit Analysis Table in Communication Manager, 911 must be administered to be call type emer or alrt for the E911 Emergency feature to work properly.

Message Lamp Ext

The extension of the station tracked with the message waiting lamp.

Lock Messages

Controls access to voice messages by other users.

Valid Entry	Usage
y	Restricts other users from reading or canceling the voice messages, or retrieving messages using Voice Message Retrieval.
n	Allows other users to read, cancel, or retrieve messages.

Feature Options

This section lets you set features unique to a particular voice terminal type.

Location

This field appears only when the **Multiple Locations** field is set to y and the **Type** field is set to H.323 or SIP station types.

Valid entry	Usage
1 to 250	(Depending on your server configuration, see *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.) Assigns the location number to a particular station. Allows IP telephones and softphones connected through a VPN to be associated with the branch an employee is assigned to. This field is one way to associate a location with a station. For the other ways and for a list of features that use location, see the Location sections in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.
blank	Indicates that the existing location algorithm applies. By default, the value is blank.

DTMF Over IP

Specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling. Available only if **Group Type** is sip.

Valid Entry	Usage
in-band	All G711 and G729 calls pass DTMF in-band. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G.723 is sent out-of-band.
in-band-g711	Only G711 calls pass DTMF in-band.

Valid Entry	Usage
out-of-band	All IP calls pass DTMF out-of-band. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This value is not supported for SIP signaling. This is the default for newly added H.323 signaling groups.
rtp-payload	This method is specified by RFC 2833. By default, RFC 2833 is the default value for newly added SIP signaling groups. Support for SIP trunks requires the default entry of rtp-payload.

Active Station Ringing

Defines how calls ring to the telephone when it is off-hook without affecting how calls ring at this telephone when the telephone is on-hook.

Valid Entry	Usage
continuous	All calls to this telephone ring continuously.
single	Calls to this telephone receive one ring cycle and then ring silently.
if-busy-single	Calls to this telephone ring continuously when the telephone is off-hook and idle. Calls to this telephone receive one ring cycle and then ring silently when the telephone is off-hook and active.
silent	All calls to this station ring silently.

Auto Answer

In EAS environments, the auto answer setting for the Agent LoginID can override a station’s setting when an agent logs in.

Valid Entry	Usage
all	All ACD and non-ACD calls terminated to an idle station cut through immediately. Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when the **Allow Ringer-off with Auto-Answer** is enabled for the system.
acd	Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls terminated to a station ring audibly. For analog stations, the station is off-hook and idle, only the ACD split/ skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the station is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone.
none	All calls terminated to this station receive an audible ringing treatment.
icom	Allows a telephone user to answer an intercom call from the same intercom group without pressing the **intercom** button.

MWI Served User Type

Controls the auditing or interrogation of a served user’s message waiting indicator (MWI).

Valid Entries	Usage
fp-mwi	The station is a served user of an fp-mwi message center.
qsig-mwi	The station is a served user of a qsig-mwi message center.
blank	The served user's MWI is not audited or if the user is not a served user of either an fp-mwi or qsig-mwi message center.

Coverage After Forwarding

Governs whether an unanswered forwarded call is provided coverage treatment.

Valid Entry	Usage
y	Coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters.
n	No coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters.
s(ystem)	Administered system-wide coverage parameters determine treatment.

Per Station CPN - Send Calling Number

Determines Calling Party Number (CPN) information sent on outgoing calls from this station.

Valid Entries	Usage
y	All outgoing calls from the station deliver the CPN information as "Presentation Allowed."
n	No CPN information is sent for the call.
r	Outgoing non-DCS network calls from the station delivers the Calling Party Number information as "Presentation Restricted."
blank	The sending of CPN information for calls is controlled by administration on the outgoing trunk group the calls are carried on.

Display Language

Valid Entry	Usage
english french italian spanish user-defined	The language that displays on stations. Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.).
unicode	Displays English messages in a 24-hour format . If no Unicode file is installed, displays messages in English by default. **Note:** Unicode display is only available for Unicode-supported telephones. Currently, 4610SW, 4620SW, 4621SW, 4622SW, 16xx, 96xx, 96x1, and 9600-series telephones (Avaya one-X Deskphone Edition SIP R2

Valid Entry	Usage
	or later) support Unicode display. Unicode is also an option for DP1020 (aka 2420J) and SP1020 (Toshiba SIP Phone) telephones when enabled for the system.

Personalized Ringing Pattern

Defines the personalized ringing pattern for the station. Personalized Ringing allows users of some telephones to have one of 8 ringing patterns for incoming calls. For virtual stations, this field dictates the ringing pattern on its mapped-to physical telephone.

L = 530 Hz, M = 750 Hz, and H = 1060 Hz

Valid Entries	Usage
1	MMM (standard ringing)
2	HHH
3	LLL
4	LHH
5	HHL
6	HLL
7	HLH
8	LHL

Hunt-to Station

The extension the system should hunt to for this telephone when the telephone is busy. A station hunting chain can be created by assigning a hunt-to station to a series of telephones.

Remote Softphone Emergency Calls

TellsCommunication Manager how to handle emergency calls from the IP telephone.

⚠ **Caution:**

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. Please be advised that an Avaya IP endpoint cannot dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. Do not use an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones.

Available only if the station is an IP Softphone or a remote office station.

Valid Entry	Usage
as-on-local	If the emergency location extension that corresponds to this station's IP address is not administered (left blank), the value as-on-local sends the station emergency location extension to the Public Safety Answering Point (PSAP). If the administrator populates the IP address mapping with emergency numbers, the value as-on-local functions as follows: • If the station emergency location extension is the same as the IP address mapping emergency location extension, the value as-on-local sends the station's own extension to the Public Safety Answering Point (PSAP). • If the station emergency location extension is different from the IP address mapping emergency location extension, the value as-on-local sends the IP address mapping extension to the Public Safety Answering Point (PSAP).
block	Prevents the completion of emergency calls. Use this entry for users who move around but always have a circuit-switched telephone nearby, and for users who are farther away from the server than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP Telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.
cesid	Allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. The end user enters the emergency information into the IP Softphone. Use this entry for IP Softphones with road warrior service that are near enough to the server that an emergency call routed over the it's trunk reaches the PSAP that covers the server or switch. If the server uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the server uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP Softphone location, based on advice from the local emergency response personnel.
option	Allows the user to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported. This entry is used for extensions that can be swapped back and forth between IP Softphones and a telephone with a fixed location. The user chooses between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects the extension.

Service Link Mode

Determines the duration of the service link connection. The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and a server running Avaya Communication Manager that terminates the H.320 protocol. When the user receives or makes a call during a multimedia or IP Softphone or IP Telephone session, a “service link” is established.

Valid Entry	Usage
as-needed	Used for most multimedia, IP Softphone, or IP Telephone users. Setting the Service Link Mode to as-needed leaves the service link connected for 10 seconds after the user ends a call so that they can immediately place or take another call. After 10 seconds the link is dropped and a new link would have to be established to place or take another call.
permanent	Used for busy call center agents and other users who are constantly placing or receiving multimedia, IP Softphone, or IP Telephone calls. In permanent mode, the service link stays up for the duration of the multimedia, IP Softphone, or IP Telephone application session.

Loss Group

Valid Entry	Usage
1 to 17	Determines which administered two-party row in the loss plan applies to each station. Does not appear for stations that do not use loss — such as x-mobile stations and MASI terminals.

Speakerphone

Controls the behavior of speakerphones.

Valid Entry	Usage
1-way	Indicates that the speakerphone listen-only.
2-way	Indicates that the speakerphone is both talk and listen.
grp-listen	Group Listen allows a telephone user to talk and listen to another party with the handset or headset while the telephone’s two-way speakerphone is in the listen-only mode. Others in the room can listen, but cannot speak to the other party through the speakerphone. The person talking on the handset acts as the spokesperson for the group. Group Listen provides reduced background noise and improves clarity during a conference call when a group needs to discuss what is being communicated to another party. Available only with 6400-series and 2420/2410 telephones.
none	Not administered for a speakerphone.

LWC Reception

Indicates where Leave Word Calling (LWC) messages are stored.

Valid Entry	Usage
audix	LWC messages are stored on the voice messaging system.
none	LWC messages are not be stored.
spe	LWC messages are stored in the system or on the switch processor element (spe).

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.

Time of Day Lock Table

Valid Entry	Usage
1 to 5	Assigns the station to a Time of Day (TOD) Lock/Unlock table. The assigned table must be administered and active.
blank	Indicates no TOD Lock/Unlock feature is active. This is the default.

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.

Media Complex Ext

When used with Multi-media Call Handling, indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to place either a voice or a data call, and voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.

Valid Entry	Usage
A valid BRI data extension	For MMCH, enter the extension of the data module that is part of this multimedia complex.
H.323 station extension	For 4600 series IP Telephones, enter the corresponding H.323 station. For IP Softphone, enter the corresponding H.323 station. If you enter a value in this field, you can register this station for either a road-warrior or telecommuter/Avaya IP Agent application.
blank	Leave this field blank for single-connect IP applications.

AUDIX Name

The voice messaging system associated with the station. Must contain a user-defined adjunct name that was previously administered.

Call Appearance Display Format

Specifies the display format for the station. Bridged call appearances are not affected by this field. This field is available only on telephones that support downloadable call appearance buttons, such as the 2420 and 4620 telephones.

Note:

This field sets the administered display value only for an individual station.

Valid Entry	Usage
loc-param-default	The system uses the administered system-wide default value. This is the default.
inter-location	The system displays the complete extension on downloadable call appearance buttons.
intra-location	The system displays a shortened or abbreviated version of the extension on downloadable call appearance buttons.

IP Phone Group ID

Available only for H.323 station types.

Valid Entry	Usage
0 to 999 blank	The Group ID number for this station.

Always Use

Enables or disables the following emergency call handling settings:

- A softphone can register no matter what emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the administered **Emergency Location Extension** is used. The softphone's user-entered settings are ignored.
- If an IP telephone dials 911, the administered **Emergency Location Extension** is used.
- If a call center agent dials 911, the physical station extension is displayed, overriding the administered **LoginID for ISDN Display** .

Does not apply to SCCAN wireless telephones, or to extensions administered as type h.323.

Audible Message Waiting

Enables or disables an audible message waiting tone indicating the user has a waiting message consisting of a stutter dial tone when the user goes off-hook.

This field does *not* control the Message Waiting lamp.

Available only if **Audible Message Waiting** is enabled for the system.

Auto Select Any Idle Appearance

Enables or disables automatic selection of any idle appearance for transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Communication Manager selects the first idle appearance.

Bridged Call Alerting

Controls how the user is alerted to incoming calls on a bridged appearance.

Valid Entry	Usage
y	The bridged appearance rings when a call arrives at the primary telephone.
n	The bridged appearance flashes but does not ring when a call arrives at the primary telephone. This is the default. If disabled and **Per Button Ring Control** is also disabled, audible ringing is suppressed for incoming calls on bridged appearances of another telephone’s primary extension.

Bridged Idle Line Preference

Specifies whether the selected line for incoming bridged calls is always an idle line.

Valid Entry	Usage
y	The user connects to an idle call appearance instead of the ringing call.
n	The user connects to the ringing call appearance.

CDR Privacy

Enables or disables Call Privacy for each station. Allows digits in the called number field of an outgoing call record to be blanked on a per-station basis. The number of blocked digits is administered system-wide as CDR parameters.

Conf/Trans On Primary Appearance

Enables or disables the forced use of a primary appearance when the held call to be conferenced or transferred is a bridge. This is regardless of the administered value for **Auto Select Any Idle Appearance** .

Coverage Msg Retrieval

Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.

IP Video

Enables or disables IP video capability for this signaling group. Available only if the signaling group type h.323 and sip.

Data Restriction

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

Direct IP-IP Audio Connections

Allows or denies direct audio connections between IP endpoints that saves on bandwidth resources and improves sound quality of voice over IP transmissions.

Display Client Redirection

Enables or disables the display of redirection information for a call originating from a station with Client Room Class of Service and terminating to this station. When disabled, only the client name and extension or room display. Available only if Hospitality is enabled for the system.

Note:

This field must be enabled for stations administered for any type of voice messaging that needs display information.

Select Last Used Appearance

Valid Entry	Usage
y	Indicates a station's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. The line selection on an on-hook station only moves from the last used line button to a line button with an audibly alerting call. If there are no alerting calls, the line selection remains on the button last used for a call.
n	The line selection on an on-hook station with no alerting calls can be moved to a different line button that might be serving a different extension.

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.

H.320 Conversion

Enables or disables the conversion of H.320 compliant calls made to this telephone to voice-only. Because the system can handle only a limited number of conversion calls, the number of telephones with H.320 conversion should be limited.

Idle Appearance Preference

Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.

Valid Entry	Usage
y	The user connects to an idle call appearance instead of the ringing call.
n	The Alerting Appearance Preference is set and the user connects to the ringing call appearance.

IP Audio Hairpinning

Enables or disables hairpinning for H.323 or SIP trunk groups. H.323 and SES-enabled endpoints are connected through the IP circuit pack without going through the time division multiplexing (TDM) bus. Available only if **Group Type** is h.323 or sip.

IP Softphone

Indicates whether or not this extension is either a PC-based multifunction station or part of a telecommuter complex with a call-back audio connection.

Available only for DCP station types and IP Telephones.

LWC Activation

Activates or deactivates the Leave Word Calling (LWC) feature. LWC allows internal telephone users on this extension to leave short pre-programmed messages for other internal users.

LWC should be used if:

- The system has hospitality and the guest-room telephones require LWC messages indicating that wakeup calls failed
- LWC messages are stored in a voice-messaging system

LWC Log External Calls

Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls provided information on the caller identification is available. Each record consists of the latest call attempt date and time.

Multimedia Early Answer

Enables or disables multimedia early answer on a station-by-station basis.

The station should be enabled for this feature if the station receives coverage calls for multimedia complexes, but is not multimedia-capable. This ensures that calls are converted and the talk path is established before ringing at this station.

Mute Button Enabled

Enables or disables the mute button on the station.

Per Button Ring Control

Enables or disables per button ring control by the station user.

Valid Entries	Usage
y	Allows users to select ring behavior individually for each call-appr, brdg-appr, or abrdg-appr on the station and to enable Automatic Abbreviated and Delayed ring transition for each call-appr on the station. Prevents the system from automatically moving the line selection to a silently alerting call unless that call was audibly ringing earlier.
n	Calls on **call-appr** buttons always ring the station and calls on **brdg-appr** or **abrdg-appr** buttons always ring or not ring based on the **Bridged Call Alerting** value. Allows the system to move line selection to a silently alerting call if there is no call audibly ringing the station.

Precedence Call Waiting

Activates or deactivates Precedence Call Waiting for this station.

Redirect Notification

Enables or disables redirection notification that gives a half ring at this telephone when calls to this extension are redirected through Call Forwarding or Call Coverage. Must be enabled if LWC messages are stored on a voice-messaging system.

Restrict Last Appearance

Valid Entries	Usage
y	Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only.
n	Last idle call appearance is used for incoming priority calls and outgoing call originations.

EMU Login Allowed

Enables or disables using the station as a visited station by an Enterprise Mobility User (EMU).

Bridged Appearance Origination Restriction

Restricts or allows call origination on the bridged appearance.

Valid Entry	Usage
y	Call origination on the bridged appearance is restricted.
n	Call origination ion the bridged appearance is allowed. This is normal behavior, and is the default.

Voice Mail Number

The complete Voice Mail Dial Up number. Accepts up to 17 digits.

Site Data

This section lets you set information about the Room, Floor, Jack, Cable, Mounting, and Building.

Room

Valid Entry	Usage
Telephone location	Identifies the telephone location. Accepts up to 10 characters.
Guest room number	Identifies the guest room number if this station is one of several to be assigned a guest room and the **Display Room Information in Call Display** is enabled for the system. Accepts up to five digits.

Floor

A valid floor location.

Jack

Alpha-numeric identification of the jack used for this station.

Cable

Identifies the cable that connects the telephone jack to the system.

Mounting

Indicates whether the station mounting is d(esk) or w(all).

Building

A valid building location.

Set Color

Indicates the set color. Valid entries include the following colors: beige, black, blue, brown, burg (burgundy), gray, green, ivory, orng (orange), red, teak, wal (walnut), white, and yel (yellow).

You can change the list of allowed set colors by using the Valid Set Color fields on the site-data screen.

Cord Length

The length of the cord attached to the receiver. This is a free-form entry, and can be in any measurement units.

Headset

Indicates whether or not the telephone has a headset.

Speaker

Indicates whether or not the station is equipped with a speaker.

Abbreviated Call Dialing

This section lets you create abbreviated dialing lists for a specific station, and provide lists of stored numbers that can be accessed to place local, long-distance, and international calls; allows you to activate features or access remote computer equipment and select enhanced, personal, system or group lists.

Abbreviated Dialing List 1, List 2, List 3

Assigns up to three abbreviated dialing lists to each telephone.

Valid Entry	Usage
enhanced	Allows the telephone user to access the enhanced system abbreviated dialing list.
group	Allows the telephone user to access the specified group abbreviated dialing list. Requires administration of a group number.
personal	Allows the telephone user to access and program their personal abbreviated dialing list. Requires administration of a personal list number.
system	Allows the telephone user to access the system abbreviated dialing list.

Personal List

Establishes a personal dialing list for telephone or data module users. The personal list must first be assigned to the telephone by the System Administrator before the telephone user can add entries in the list. Users access the lists in order to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `change abbreviated-dialing personal`

Abbreviated Dialing Enhanced List

Establishes system-wide or personal lists for speed dialing.

The Enhanced Abbreviated Dialing List can be accessed by users to place local, long-distance, and international calls; to activate or deactivate features; or to access remote computer equipment.

Note:

Dialing must be enabled in the license file before the Enhanced List can be programmed.

Example command: `display abbreviated-dialing enhanced`

Group List

Implements the Abbreviated Dialing Group List. The System Administrator controls the Group Lists. Up to 100 numbers can be entered for every group list. Users can access this list to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `change abbreviated-dialing group`

Enhanced Call Fwd

This section allows you to specify the destination extension for the different types of call forwards.

Forwarded Destination

A destination extension for both internal and external calls for each of the three types of enhanced call forwarding (Unconditional, Busy, and No Reply). Accepts up to 18 digits. The first digit can be an asterisk *.

Requires administration to indicate whether the specific destination is active (enabled) or inactive (disabled).

SAC/CF Override

Allows the user of a station with a **Team** button administered, who is monitoring another station, to directly reach the monitored station by pushing the **Team** button. This overrides any currently active rerouting, such as Send All Calls and Call Forwarding, on the monitored station.

Valid Entries	Usage
Ask	The system asks if the user wants to follow the rerouting or override it. When the user has the option to decide whether rerouting should take place or not, a message is sent to the station that displays the active rerouting and the number of the forwarded to station.
No	Cannot override rerouting. The station does not have the ability to override the rerouting of a monitored station.
Yes	Can override rerouting. The station has the ability to override the rerouting the monitored station has set, as long as one incoming call appearance is free.

Button Assignment

This section lets you assign features to the buttons on a phone. You can assign the main buttons for your station by choosing an option from the list down box for each button.

Group Membership

This section describes the different groups that an extension can be a member of. You should select the station you want to group and then choose the group from the drop-down box, before clicking **Commit**.

Understanding groups

Your voice system uses groups for a number of different purposes. This topic describes the different groups that an extension can be a member of. However, your voice system may include other types of groups as well (for example, trunk groups). For information on those groups, see the Administrator's Guide to Communication Manager Software.

Your voice system may have any of the following types of groups set up:

Type	Description
group page	Group page is a feature that allows you to make an announcement to a pre-programmed group of phone users. The announcement is heard through the speakerphone built into some sets. Users will hear the announcement if their set is idle. Users cannot respond to the announcement.

coverage answer group	A coverage answer group lets up to 8 phones ring simultaneously when a call is redirected to the group.
coverage path	A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call. For more information on coverage paths, see "Creating Coverage Paths" in the Administrator's Guide to Communication Manager Software.
hunt group	A hunt group is a group of extensions that receive calls according to the call distribution method you choose. When a call is made to a certain phone number, the system connects the call to an extension in the group. Use hunt groups when you want more than one person to be able to answer calls to the same number. For more information on hunt groups, see "Managing Hunt Groups" in the Administrator's Guide to Communication Manager Software.
intercom group	An intercom group is a group of extensions that can call each other using the intercom feature. With the intercom feature, you can allow one user to call another user in a predefined group just by pressing a couple of buttons. For more information on intercom groups, see "Using Phones as Intercoms" in the Administrator's Guide to Communication Manager Software.
pickup group	A pickup group is a group of extensions in which one person may pick up another person's calls. For more information on pickup groups, see "Adding Call Pickup" in the Administrator's Guide to Communication Manager Software.
terminating extension group	A Terminating Extension Group (TEG) allows an incoming call to ring as many as 4 phones at one time. Any user in the group can answer the call. For more information on terminating extension groups, see "Assigning a Terminating Extension Group" in the Administrator's Guide to Communication Manager Software.

Subscriber Templates (CMM) field descriptions

Field	Description
Template name	Specifies the template of this subscriber template.
New Template Name	Specifies the name of the duplicate template. You can enter the name of your choice.
Type	Specifies the messaging type of the subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local machine.
Password	The default password that a user has to use to login to his/her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.

Field	Description
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Reset	Undoes all the changes.
Edit	Allows you to edit the fields.
Done	Completes your action and takes you to the previous page.
Cancel	Takes you to the previous page.

Subscriber Templates (MM) field descriptions

Field	Description
Type	Specifies the messaging type of the subscriber template.
New Template Name	Specifies the name of the duplicate template. You can enter the name of your choice.
Template name	Specifies the messaging template of a subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
Class Of Service	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]) .
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent

Field	Description
	messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: to allow the subscriber to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Reset	Undoes all the changes.
Edit	Allows you to edit the fields.
Done	Completes your action and takes you to the previous page.
Cancel	Takes you to the previous page.

Chapter 26: Subscribers

Subscriber Management

System Manager lets you perform selected messaging system administration activities. You can add, view, edit, and delete subscribers through System Manager. Apart from subscriber management, you can also administer mailboxes and modify mailbox settings for a messaging system.

System Manager supports:

- Communication Manager 5.0 and later
- Avaya Aura™ Messaging 6.0
- Avaya Aura™ Modular Messaging 5.0 and later
- Communication Manager Messaging 5.2 (with LDAP support) and later

Adding a subscriber

Procedure

1. On the System Manager console, under **Elements**, click **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. From the list of messaging systems, select one or more messaging systems.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions**, and **Miscellaneous** sections.
7. Complete the **Add Subscriber** page and click **Commit** to add the subscriber.

   Note:

   If you select more than one Messaging, Modular Messaging, or Communication Manager Messaging from the list of messaging systems, and then click **New**, the system displays the Add Subscriber page with the first Messaging, Modular Messaging, or Communication Manager Messaging in context.

Related topics:

[Subscribers (Messaging) field descriptions](#) on page 721
[Subscribers (CMM) field descriptions](#) on page 725
[Subscribers (MM) field descriptions](#) on page 728

Editing a subscriber

Procedure

1. On the System Manager console, under **Elements**, click **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. From the list of messaging systems, select a messaging system.
4. Click **Show List**.
5. From the subscriber list choose the subscriber you want to edit.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields in the **Edit Subscriber** page.
8. Click **Commit** to save the changes.

Related topics:

[Subscribers (Messaging) field descriptions](#) on page 721
[Subscribers (CMM) field descriptions](#) on page 725
[Subscribers (MM) field descriptions](#) on page 728

Viewing a subscriber

Procedure

1. On the System Manager console, under **Elements**, click **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. From the list of messaging systems, select a messaging system.

4. Click **Show List**.
5. From the subscriber list, select the subscriber you want to view.
6. Click **View**.

   Note:

   You cannot edit any field on the View Subscriber page.

Related topics:

[Subscribers (Messaging) field descriptions](#) on page 721
[Subscribers (CMM) field descriptions](#) on page 725
[Subscribers (MM) field descriptions](#) on page 728

Deleting a subscriber

Procedure

1. On the System Manager console, under **Elements**, click **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of messaging systems.
4. Click **Show List**.
5. From the subscriber list, select the subscribers you want to delete.
6. Click **Delete**.
   The system displays a confirmation page for deleting the subscriber.
7. Confirm to delete the subscriber or subscribers.

   Note:

   You cannot delete a subscriber associated with a user through mailbox management. You can delete the user associated subscribers only through User Profile Management.

Subscriber List

Subscriber List displays all the subscribers under a messaging version (Messaging, Communication Manager Messaging, or Modular Messaging). You can apply filters to each column in the Subscriber List. You can also sort the subscribers according to each of the column in the Subscriber List. When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Name	Specifies the name of the subscriber.
Mailbox Number	Specifies the mailbox number of the subscriber.
Email Handle	Specifies the e-mail handle of the subscriber.
Telephone Number	Specifies the telephone number of the mailbox.
Last Modified	Specifies the time and date when the subscriber details were last modified.
User	If a subscriber is associated with a user, then the system displays the name of the user in this column.
System	Specifies the messaging system of the subscriber.

Filtering subscribers

Procedure

1. On the System Manager console, under **Elements**, click **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. From the list of messaging systems, select one of the supported messaging version.
4. Click **Show List**.
5. Click the **Filter: Enable** option in the Subscriber List.
6. Filter the subscribers according to one or multiple columns.
7. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

   Note:

   The table displays only those subscribers that match the filter criteria.

Subscribers (Messaging) field descriptions

Field	Description
Type	Specifies the messaging type of the subscriber template.
Template Name	Specifies the messaging template of a subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
Class Of Service	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]).
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII version of name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Subscriber Security

Field	Description
Expire Password	Specifies whether your password expires or not. You can choose one of the following: • **yes**: for password to expire • **no**: if you do not want your password to expire
Is Mailbox Locked?	Specifies whether you want your mailbox to be locked. A subscriber mailbox can become locked after two unsuccessful login attempts. You can choose one of the following: • **no**: to unlock your mailbox • **yes**: to lock your mailbox and prevent access to it

Mailbox Features

Field	Description
Personal Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this

Field	Description
	subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
VoiceMail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-

Field	Description
	answer messages from other subscribers. You can choose one of the following: • **yes**: to allow the subscriber to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary Extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Miscellaneous 1	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 2	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 3	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 4	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Saves all the changes.
Reset	Undoes all the changes.
Cancel	Takes you to the previous page.

Subscribers (CMM) field descriptions

Field	Description
System	Specifies the messaging system of the subscriber you want to add.
Template	Specifies the template for this subscriber. You can choose any template from the drop-down box.
Type	Specifies the messaging type of your subscriber.
Software Version	Specifies the messaging version of the subscriber.
Save as Template	Saves your current settings as a template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local machine.
Password	The default password that a user has to use to login to his/her mailbox. The password you

Field	Description
	enter can be 1 to 15 digits in length and cannot be blank
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber to the messaging system.
Schedule	Adds the subscriber at the specified time.
Save as Template	Saves the settings as a template.

Button	Description
Reset	Clears all the changes.
Edit	Allows you to edit the fields.
Done	Completes your action and takes you to the previous page.
Cancel	Takes you to the previous page.

Subscribers (MM) field descriptions

Field	Description
System	Specifies the messaging system of the subscriber you want to add. You can choose this option from the drop-down box.
Type	Specifies the messaging type of your subscriber.
Template	Specifies the messaging template of a subscriber. You can choose an option from the drop-down box.
Software Version	Specifies the message version of the subscriber.
Save as Template	Saves your current settings as a template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such

Field	Description
	as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]).
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Subscriber Security

Field	Description
Expire Password	Specifies whether your password expires or not. You can choose one of the following: • **yes**: for password to expire • **no**: if you do not want your password to expire
Is Mailbox Locked?	Specifies whether you want your mailbox to be locked. A subscriber mailbox can become locked after two unsuccessful login attempts. You can choose one of the following: • **no**: to unlock your mailbox • **yes**: to lock your mailbox and prevent access to it

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent

Field	Description
	messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: to allow the subscriber to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber to the messaging system.
Schedule	Adds the subscriber at the specified time.
Save as Template	Saves the settings as a template.
Reset	Clears all your changes.
Edit	Allows you to edit all the fields.
Done	Completes your current action and takes you to the previous page.
Cancel	Takes you to the previous page.

Chapter 27: Discovery Management

Discovery Management

Discovery Management

The Discovery Management feature allows you to configure System Manager to discover specific devices within the network. This feature also lets you manage the SNMP access parameters used for the discovery process.

Device Discovery detects or discovers your network, including subnets and nodes. Device Discovery exclusively uses Simple Network Management Protocol (SNMP) to discover your network.

Device Discovery in System Manager includes:

- Configuring SNMP access parameters, Communication Manager access parameters and subnets
- Discovering the devices
- Populating the devices discovered in the Network Device Inventory list

SNMP Access list

You can use the SNMP Access list to configure the basic SNMP parameters for specific devices or for a range of devices. **Discovery Management** recognizes SNMP V1 and V3 protocols. For both these protocols access parameters also include timeout and retry values.

Name	Description
Type	Specifies the SNMP protocol type. Value can either be V1 or V3.
Read Community	The read community of the device. Only applicable for SNMP V1 protocol.
Write Community	The write community of the device. Only applicable for SNMP V1 protocol.

Name	Description
User	User name as defined in the application. Applicable for SNMP V3 protocol only.
Auth Type	The authentication protocol used to authenticate the source of traffic from SNMP V3 protocol users. Possible values are: • **MD5 (default)** • **SHA** Authorization Type is applicable only for SNMP V3 protocol.
Priv Type	The encryption policy for SNMP V3 users. Possible values are: • **DES**: Use DES encryption for SNMP based communication. • **AES**: Use AES encryption for SNMP based communication • **No Privacy**: Do not encrypt traffic for this user Privacy Type is applicable only for SNMP V3 users.
Timeout (ms)	The number of milliseconds discovery waits for the response from the device being polled.
Retries	The number of times discovery polls a device without receiving a response before timing out.
Description	Describes the SNMP Access profile.

Setting the order in the SNMP Access list

About this task

You can set the order in which you want to list the SNMP Access profiles in the SNMP Access list. While polling a device, the SNMP Access profiles are used according to this list.

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. Select the SNMP Access profile you want to move up or move down.

4. Do one of the following:
    - Click **Move Up** if you want to set the SNMP Access profile one step ahead in the list.
    - Click **Move Down** if you want to set the SNMP Access profile one step down in the list.

Related topics:
SNMP Access list on page 733

Adding an SNMP Access profile

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. Click **New**.
4. Select the SNMP protocol type from the **Type** field.
5. Complete the **Add SNMP Access Configuration** page and click **Commit**.

Related topics:
SNMP Access field descriptions on page 736

Editing an SNMP Access profile

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. Select the SNMP Access profile you want to edit.
4. Click **Edit**.
5. Edit the required fields on the **Edit SNMP Access Configuration** page.
6. Click **Commit** to save the changes.

Related topics:
SNMP Access field descriptions on page 736

Deleting an SNMP Access profile

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. Select the SNMP Access profiles you want to delete.
4. Click **Delete**.
5. Confirm to delete the SNMP Access profiles.

SNMP Access field descriptions

For SNMP protocol V3

Name	Description
Type	Specifies the SNMP protocol type. Value can be either V1 or V3.
User	User name as defined in the application.
Authentication Type	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. Possible values are: • **MD5 (default)** • **SHA** Authorization Type is applicable only for SNMP V3 protocol.
Authentication Password	The password used to authenticate the user. Passwords must consist of at least eight characters.
Confirm Authentication Password	You must re-type the SNMP V3 protocol authentication password for confirmation.

Name	Description
Privacy Type	The encryption policy for an SNMP V3 user. Possible values are: • **DES**- Use DES encryption for SNMP based communication. • **AES**- Use AES encryption for SNMP based communication. • **No Privacy** - Do not encrypt traffic for this user. Privacy Type is only required for an SNMP V3 user.
Privacy Password	The password used to enable DES or AES encryption, if you select DES as the Privacy Type. DES Passwords must consist of at least eight characters.
Confirm Privacy Password	You must re-type the privacy password in this field for confirmation.
Timeout (ms)	The number of milliseconds discovery waits for the response from the device being polled.
Retries	The number of times discovery polls a device without receiving a response before timing out.

For SNMP protocol V1

Field	Description
Type	Specifies the SNMP protocol type. Value can be either V1 or V3.
Read Community	The read community of the device. Only applicable for SNMP V1 protocol.
Write Community	The write community of the device. Only applicable for SNMP V1 protocol.
Timeout (ms)	The number of milliseconds discovery waits for the response from the device being polled.
Retries	The number of times discovery polls a device without receiving a response before timing out.

Button	Description
Commit	Adds or edits the SNMP Access profile (whichever applicable).
Reset	Undoes your action.
Cancel	Takes you to the previous page.

Subnet(s) List

The Subnet(s) List contains the list of subnets that are manually added.

Name	Description
Subnet IP	IP address of the subnet.
Subnet Mask	Specifies the IP subnet mask
Use SNMP V3	Specifies whether you want to only use SNMP V3 protocol. Select the check box to only use SNMP V3 protocol.

Button	Description
Commit	Adds or edits the subnet.
Reset	Undoes all the entries.
Cancel	Cancels your current action and takes you to the previous page.

Adding a subnet

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. Click **New** in the Subnet(s) section.
4. Complete the **Add Subnet Configuration** page and click **Commit**.

Related topics:

Subnet(s) List on page 738

Editing a subnet

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. Select the subnet you want to edit.
4. Click **Edit**.
5. Edit the required fields on the **Edit Subnet Configuration** page.
6. Click **Commit** to save the changes.

Related topics:
Subnet(s) List on page 738

Deleting a subnet

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. Select the subnets you want to delete.
4. Click **Delete**.
5. Confirm to delete the subnets.

CM Access list

The CM Access list specifies the Communication Manager login parameters to connect to the Communication Manager servers in your network.

Name	Description
IP address	IP address of the Communication Manager.
Port	Login port of the Communication Manager.
Login	Login name as configured on the Communication Manager server.

Name	Description
Use ASG Key	Indicates the use of ASG encryption.
Use SSH	Indicates the use of SSH protocol.
Global profile	Specifies the default parameters that can be used to configure a Communication Manager server in the Entities application in System Manager.

Filtering Subnet(s) and CM Access lists

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. Click **Filter: Enable** in the Subnet(s) list or the CM Access list.
4. Filter the subnets or the CM access profiles according to one or multiple columns.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

   Note:

   The table displays only those options that match the filter criteria.

Adding a Communication Manager Access profile

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. On the Configuration page, click **New** in the CM Access section.
4. Complete the Add CM Access details page and click **Commit**.

Related topics:

CM Access profile field descriptions on page 741

Editing a Communication Manager Access profile

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. Select the Communication Manager Access profile you want to edit.
4. Click **Edit**.
5. Edit the required fields on the Edit CM Access details page.
6. Click **Commit** to save the changes.

Related topics:
CM Access profile field descriptions on page 741

Deleting a Communication Manager Access profile

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Configuration** in the left navigation pane.
3. Select the Communication Manager Access profile you want to delete.
4. Click **Delete**.
5. Confirm to delete the Communication Manager Access profile.

CM Access profile field descriptions

Name	Description
IP Address	IP address of the Communication Manager.
Port	Login port of the Communication Manager.
Login	Login name as configured on the Communication Manager server.
Password	Password for logging in.

Name	Description
Confirm Password	Re-enter password for confirmation.
Use ASG Key	Indicates the use of ASG encryption.
ASG key	Specifies the ASG password or key for login. ASG key is a 20 character octal code.
Use SSH	Indicates the use of SSH protocol.
Global Profile	Specifies the default parameters that can be used to configure a Communication Manager server in the Entities application in System Manager. You can select this checkbox only once. This checkbox is disabled once you configure the Global Profile.

Button	Description
Commit	Adds or edits the Communication Manager Access profile.
Reset	Undoes the current action.
Cancel	Cancels the current action and takes you to the previous page.

Discovery

Device Discovery

The **Discovery** tab in **Discovery Management** allows you to configure the subnets and device types to be discovered. You must select the subnet as well as the device type before starting the discovery process.

Discovering devices

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Discovery** on the left navigation pane.

3. Select the subnet and the device type from the Network Subnet(s) list and the Device Type(s) list respectively.
4. Click **Now** to start the discovery process.

   ✱ **Note:**

   To schedule the discovery process at a later time, click **Schedule**.

   ✱ **Note:**

   To restart the discovery process, select the **Clear previous results** check box. When you select this check box, the discovered devices are removed only from the inventory list and not from the Entities application.

Related topics:
Discovering Devices field descriptions on page 743

Filtering Network Subnet(s)

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovery Management** > **Discovery** in the left navigation pane.
3. Click **Filter: Enable** in the Network Subnet(s) list.
4. Filter the network subnet(s) according to one or multiple columns.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

   ✱ **Note:**

   The table displays only those options that match the filter criteria.

Discovering Devices field descriptions

Select Network Subnet list

Name	Description
Subnet IP	IP address of the subnet.

Name	Description
Subnet Mask	Specifies the subnet mask.
Use SNMP V3	Specifies whether you want to only use SNMP V3 protocol. Select the checkbox to only use the SNMP V3 protocol.
Discovery Status	Provides information about the current discovery status. Possible values include: • **Pending** • **In Progress** • **In Progress: preparing for discovery** • **In Progress: probing network elements** • **In progress: saving discovered elements** • **In progress: collecting inventory information** • **In progress: saving inventory information** • **Failed** • **Idle**
Last Discovered Time	Latest time when the discovery was carried out.

Select Device Type list

Name	Description
Device Type	Specifies the type of the device.
Description	Describes the device type.

Discovered Inventory

Discovered Inventory

The **Discovered Inventory** tab displays a list of all the inventory components or items that are discovered. After the discovery is complete, the system lists the discovered devices. You can either choose the **Tree** View or the **List** View for viewing all the discovered devices.

Network Device Inventory list

The Network Device Inventory list displays all the inventory components or items that are discovered. This list also displays some of the properties of the devices discovered. You can sort this list according to any of the columns in the list.

There are two default views of the Network Device Inventory list: List View and Tree View.

- The List View lists every entity that is discovered. In this view, each entity appears as a separate row.
- The Tree View displays the inventory items in groups. The inventory items are grouped by the device type.

Related topics:

Network Device Inventory list field description on page 747

Viewing the Network Device Inventory list

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovered Inventory** in the left navigation pane.
   The system displays the **Network Device Inventory** list, which gives the details of the devices discovered.

   ✱ **Note:**

   This is a read-only list.
3. Click an IP address in the inventory list to view more information about the device.

   When you click an IP address in the list, the system displays a window which gives more information about the inventory items for that IP address. This information varies according to the device you choose.

Related topics:

Network Device Inventory list field description on page 747

Filtering the Inventory list

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovered Inventory** in the left navigation pane.
3. Click **Filter: Enable** in the Discovered Inventory list.
4. Filter the list according to one or multiple columns.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

   Note:

   The table displays only those options that match the filter criteria.

Using Advanced Search in Discovered Inventory

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Discovered Inventory** on the left navigation pane.
3. On the Network Device Inventory page, click **Advanced Search**.
4. In the Criteria section, do the following:

   a. Select the search criterion from the first drop-down field.

   b. Select the operator from the second drop-down field.

   c. Enter the search value in the third field.

   If you want to add a search condition, click the plus sign (**+**) and repeat the sub steps listed in step 3.

   If you want to delete a search condition, click the minus sign (**-**) . This button is available if there is more than one search condition.

Network Device Inventory list field description

Name	Description
Family	Specifies the device family type. Possible values include Communication Manager, Media Gateway and Switches; Application and Element Managers.
IP	IP address of the device.
Name	Name of the device.
Type	Specifies the type of the device.
Module ID	Module ID of the device.
Location	Location of the device.
Serial No	Serial number of the hardware.
Software Release	Software release of the device.
Hardware Version	Hardware version of the device.

Chapter 28: Administering LDAP Directory Application

LDAP Directory Application overview

Use the LDAP Directory Application web pages to configure LDAP Directory Application to connect to an LDAP database and to customize the search experience of the user.

In Communication Manager Release 6.0 and later, Directory Application is part of Utility Server. You can install Directory Application on the Avaya S8300D, S8510, S8800, HP DL360 G7, and Dell R610 servers.

Directory Application is available in the **Administration** menu of Avaya Aura® Utility Server System Management Interface (SMI).

The 46xx, 96xx, and 96x1 telephones use Wireless Markup Language (WML) browsers to browse LDAP databases.

Configuring Directory Application

About this task

Configure Directory Application so that users can use WML browsers to perform search operations.

Procedure

1. To start Directory Application, go to **Avaya Aura Utility Server System Management Interface (SMI)** > **Administration** > **Directory Application** .
2. On the General Settings page, specify the LDAP settings.
3. To ensure that the Directory Application can connect to the LDAP database, click **Test Connection**.
4. Enable the Directory Application for HTTP and HTTPS traffic.
5. (Optional) To customize the Search screen for the telephone browser, use the Search Screen Settings section.

6. (Optional) To customize the Details screen for the telephone browser, use the Details Screen Settings section.
7. (Optional) To customize the LDAP filter attributes, use the Ldap Filter Settings section.

Communication Manager station synchronization with the LDAP directory

Use the **Export to LDAP directory** field on the Avaya Site Administration (ASA) interface to export data from the station fields to the LDAP database. The ASA tool also provides a scheduling feature, which you can use to export data according to a schedule.

46xx and 96xx telephones URL configuration

You can configure the URL on 46xx and 96xx telephones by using the WMLHOME property in the settings file. Use the following URLs:

- The URL for HTTP is: `http://<Utility Server IP address>/directoryclient/search.php`
- The URL for HTTPS is: `https://<Utility Server IP address>/directoryclient/search.php`

For more information on configuring WML browsers for the 46xx and 96xx telephones, see *4600 Series IP Telephone LAN Administrator Guide* and *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide*.

Chapter 29: Administering IP DECT

IP DECT

Use the IP DECT (Digital Enhanced Cordless Telecommunications) feature to support an IP DECT system, an IP-based cordless telephony and messaging system for connection to private telephone exchanges.

Enabling multiple locations for IP DECT

About this task

Important:

Perform this task only if you need to enable the multiple locations feature in Communication Manager system.

Procedure

1. Enter `display system-parameters customer-options`.
2. Click **Next** until you see the **Multiple Locations** field.
3. Ensure that the **Multiple Locations** field is set to y.

   Note:

   If the **Multiple Locations** field is set to n, multiple locations is not enabled for the IP DECT feature. Contact your Avaya representative for assistance.
4. Select **Enter** to exit the screen.

Verifying system capacities

Procedure

1. Enter `display capacity`.
2. Click **Next** until you see the **Total Licensed Capacity** section.

3. Ensure that the following fields display the current information:
    - **XMOBILE Stations**: Total number of X-Mobile stations including the IP DECT stations.
    - **ISDN DECT**: Current number of ISDN-based DECT X-Mobile stations.
    - **IP DECT**: Current number of IP-based DECT X-Mobile stations.
4. Select **Enter** to exit the screen.

Assigning the codec

Procedure

1. Enter `change ip-codec-set n`, where *n* is the IP codec set number.

    ✱ **Note:**

    The codec set that has to be configured in the IP Network Region must be linked to this IP codec set screen.
2. Fill in the following fields:
    - **Audio Codec**: G.711 a-law and u-law (for 10, 20, 30 ms packets), G.729/G.729a/G.729b/G.729ab (for 10, 20, 30, 40, 50, 60 ms packets), and G.723 (for 30, 60 ms packets) depending on the audio codec used for this codec set.

        ✱ **Note:**

        When using G.729 codecs, for outgoing packets, the legacy IP DECT system (ADMM) either uses G.729A or G.729AB.
    - **Silence Suppression**: `y` or `n` depending on the codec you have set.

        The ADMM system does not support silence suppression for G.729 or G.729A codecs.
    - **Frame Per Pkt**: `2`.
    - **Media Encryption**: `none`.
3. Select **Enter** to save your changes.

    For information on administering the IP codec sets, see the Administering IP Codec sets section of *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

Configuring the network region

Procedure

1. Enter `change ip-network-region n`, where *n* is the network region.

   ✱ **Note:**

   The Far-end Network Region that has to be configured in the signaling-group must be linked to this codec.

2. Fill in the following fields:
   - **Codec Set**: 1 to 7 depending on the codec set to be used for the network region.
   - **RSVP Enabled**: `n`.

3. Click **Next** until you see the **Inter Network Region Connection Management** section.

   Avaya recommends you to use the same codec set which you already assigned, see Assigning the codec task.

   For information on administering the IP network regions, see the Administering IP network regions section of *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

4. Select **Enter** to save your changes.

Configuring the trunk group

Procedure

1. Enter `add trunk-group n`, where *n* is the trunk group number.

   ✱ **Note:**

   You must administer this trunk group to use an H.323 signaling group of x-mobility type of DECT.

2. Ensure that the **Group Type** field is set to `isdn`.

3. Fill in the following fields:
   - **Direction**: `two-way`.
   - **Carrier Medium**: `H.323`.
   - **Service Type**: `tie`.

4. Click **Next** until you see the **Trunk Parameters** section.
5. Fill in the following fields:
    - **Codeset to Send Display**: `0`.
    - **Supplementary Service Protocol**: `a`.
    - **Digit Handling (in/out)**: `overlap/enbloc`.
    - **Format**: Type the numbering format.

      The numbering format no need to be any specific type. For example, IP trunk to the IP DECT can have Private numbering format.
6. Click **Next** until you see the **Trunk Features** section.
7. Fill in the following fields:
    - **NCA-TSC Trunk Member**: 1 or higher for carrying Message Waiting Indication (MWI) facility.
    - **Send Name**: `y`.
    - **Send Calling Number**: `y`.
    - **Send Connected Number**: `y`.
8. Click **Next** until you see the **Group Member Assignments** section.
9. Add trunk group members to the numbered **Group Member Assignments**.

   Note:

   The IP DECT supports maximum of 255 simultaneous calls. The IP DECT can choose another available trunk if administered.

   Note:

   Instead of adding the trunk group members on the **Group Member Assignments**, you can set the **Member Assignment Method** field to auto.
10. Select **Enter** to save your changes.

Configuring the signaling group

Procedure

1. Enter `add signaling-group` *n*, where *n* is the signaling group number.
2. Ensure that the **Group Type** field is set to H.323.
3. Fill in the following fields:

- **Max number of NCA TSC**: 1 or higher.
- **Max number of CA TSC**: 1 or higher.
- **Trunk Group for NCA TSC**: Type the number of the previously administered or associated trunk group.
- **Trunk Group for Channel Selection**: Type the number of the previously administered or associated trunk group.
- **TSC Supplementary Service Protocol**: `a`.
- **X-Mobility/Wireless Type**: `DECT`.
- **Location for Routing Incoming Calls**: `blank` or the location of the ADMM or RFS.

  Note:

  Administer the **Location for Routing Incoming Calls** field only when the multiple locations feature is enabled for IP DECT.
- **Near-end Listen Port**: Port of the CLAN or PE.
- **Far-end Listen Port**: Port of the ADMM or RFS.
- **Far-end Network Region**: Point to the associated network region.
- **Calls Share IP Signaling Connection**: `n`.
- **Interworking Message**: `PROGress`.
- **Enable Layer 3 Test**: `y` for IP trunk supervision.

4. Select **Enter** to save your changes.

Configuring the station

Procedure

1. Enter `add station` *n*, where *n* is the extension.
2. Ensure that the **Type** field is set to XMOBILE.
3. Ensure that the **XMOBILE Type** field is set to IPDECT.
4. Fill in the following fields:
   - **Message Lamp Ext**: Type the station number.
   - **Display Module**: `y`.
   - **Message Waiting Type**: ICON, DISP, or NONE depending on the MWI message requirement.

- **Length of Display**: Type the proper length for each of the handset.

  Avaya recommends that the **Length of Display** field must be set to 16x2.
- **Mobility Trunk Group**: Type the appropriate trunk group that use the H.323 signaling groups.

  > ✱ **Note:**
  >
  > You must not change the value of the **Mobility Trunk Group** field while a call is active.
- **Mapping Mode**: `both`.

5. Select **Enter** to save your changes.