Administering Avaya Aura™ Communication Manager

03-300509
Issue 5.0
Release 5.2
May 2009

© 2009 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

To locate this document on the Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

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

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

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

http://www.avaya.com/support

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

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

http://www.avaya.com/support

Contents

About this book 9
- Overview 9
- Contents 10
- Conventions used 11
- Admonishments 12
- Trademarks 13
- Related Resources. 13
- How to obtain Avaya books on the Web 14
- How to comment on this book 15
- How to get help 15

Chapter 1: System Basics. 17
- Logging into the System 17
- Login messages 24
- Logging off the System 25
- Administering User Profiles and Logins 26
- Establishing Daylight Savings Rules. 26
- Setting Time of Day Clock Synchronization 28
- Setting the System Date and Time 34
- Using the Bulletin Board 36
- Saving Translations 38
- Performing Backups. 40

Chapter 2: Planning the System 41
- Understanding Your Configuration. 41
- Understanding the Dial Plan 42
- Controlling the features your users can access. 48
- System-wide settings 49
- Changing system parameters. 49
- Setting WAN bandwidth limits between network regions. 50
- Administering Treatment for Denied or Invalid Calls 52
- Setting up Music-on-Hold 53
- Receiving Notification in an Emergency 57
- Notifying a Digital Pager of an Emergency 59
- Other Useful Settings 61
- Controlling the Calls Your Users Can Make and Receive. 62
- Station Lock 64

Chapter 3: Managing Telephones. 69
Installing New Telephones 69
Adding new telephones 70
Duplicating telephones 75
Using an alias 76
Customizing your telephone 77
Upgrading telephones. 78
Swapping telephones 78
Using ACTR to move telephones 79
Using TTI to move telephones 81
Removing telephones 85
Adding a fax or modem 86
Adding an H.323 Softphone 88
Adding an IP telephone 92
Setting up Remote Office 96

Chapter 4: Managing Telephone Features 105
Adding Feature Buttons. 105
Telephone Feature Buttons Table 108
Adding Abbreviated Dialing Lists 131
Setting up Bridged Call Appearances 135
Setting up Extension to Cellular 137
Setting up Terminal Self-Administration 140
Setting Up Enterprise Mobility User 143

Chapter 5: Managing Attendant Consoles 149
Attendant Consoles 149
Adding an Attendant Console 154
Attendant Console Feature Buttons 155
Setting Console Parameters 162
Removing an Attendant Console 163
Providing Backup for an Attendant. 164
Return Call to (same) Attendant 165

Chapter 6: Managing Displays 167
Displaying Caller Information. 167
Displaying ANI Calling Party Information 167

Displaying ICLID Information 168
Changing the Display Language 168
Setting up Directory Buttons 178
Making Standard Telephone Features easier to use 179

Chapter 7: Handling Incoming Calls 183
Setting up Basic Call Coverage. 183
Setting up Advanced Call Coverage 186
Setting up Call Forwarding 190
Setting up Night Service 201
Adding Call Pickup 209
Managing Hunt Groups 227
Managing Vectors and VDNs 232
Understanding Automatic Call Distribution 245
Assigning a Terminating Extension Group 245

Chapter 8: Routing Outgoing Calls. 247
World Class Routing. 247
Managing Calling Privileges 247
Assigning ARS FAC 248
Displaying ARS Analysis Information 249
Understanding ARS Analysis 250
Administering Call Type Digit Analysis 255
Setting up Multiple Locations. 256
Routing with Multiple Locations 258
Modifying Call Routing 260
Overriding Call Restrictions 263
Defining ARS Partitions 264
Setting up Time of Day Routing 267
Location by Region 269

Chapter 9: Managing Multimedia Calling 271
Multimedia Applications Server Interface 271
Avaya Video Telephony Solution 297
Multimedia Call Handling 309
Understanding the Multimedia Complex 325
Enhanced Mode MM Complex 341

Chapter 10: Setting Up Telecommuting 363
Configuring Communication Manager for Telecommuting 363
Setting up Personal Station Access 365
Creating a Station Security Code 367
Assigning an Extender Password 368
Setting up Call Forwarding 370
Assigning Coverage Options 372
Installing Home Equipment 373
Setting up Remote Access 375
Changing Telecommuting Settings 378

Chapter 11: Enhancing System Security 383
Basic Security 383
Preventing Toll Fraud 384
Physical Security 386
System Security Checklist 386
Administering User Profiles and Logins 391
Using Access Security Gateway (ASG) 391
Using Busy Verify 391
Setting up Authorization Codes 392
Setting up Security Violations Notification 395
Enhanced security logging 396
Using Station Lock 397
Dealing with Security Violations 401
Hot Desking Enhancement 402

Chapter 12: Managing Trunks 405
Tips for working with trunk groups 405
Adding a CO, FX, or WATS trunk group 407
Adding a DID trunk group 410
Adding a PCOL trunk group 411
Adding a Tie or Access trunk group 414
Adding a DIOD trunk group 416
Setting up digital trunks 416
Adding trunks to a trunk group 420
Removing trunk groups 421

Resetting trunks 422
Inserting and absorbing digits 423
Administering trunks for Listed Directory Numbers 424
Administering Answer Detection 426
Administering ISDN trunk groups 427

Chapter 13: Managing Announcements 433
Getting Started with the VAL or G700 Virtual VAL 433

Chapter 14: Managing Group Communications 437
Setting up Voice Paging Over Loudspeakers 437
Setting up Chime Paging Over Loudspeakers 439
Paging Over Speakerphones 442
Paging Users Who are on Active Calls 444
Using Telephones as Intercoms 445
Setting up Automatic Answer Intercom Calls 447
Observing Calls 448

Chapter 15: Managing Data Calls 451
Types of Data Connections 451
Data Call Setup 451
Alphanumeric Dialing 458
Data Hotline 459
Data Privacy 460
Default Dialing 462
Data Restriction 462
Data-Only Off-Premises Extensions 464
Data Modules — General 465
Administered Connection 468
Modem Pooling 474
PC Interface 476
Wideband Switching 479
CallVisor Adjunct-Switch Applications Interface 490
Setting up CallVisor ASAI 492

Chapter 16: Administering Avaya Servers 493
Overview 493
Administering the G700 Media Gateway 493

Administering the Avaya S8xxx Server 498
Setting up Processor Ethernet 508
Administering the main or LSP split registration 523
Administrable Alternate Gatekeeper List for IP Phones 528
Improved Port network recovery from control network outages 542
Administering Call-processing 544
Administering Voice or Network Statistics 559
Administering SNMP 561

Chapter 17: Collecting Call Information 579
Collecting Information About Calls 579
Setting up Intra-switch CDR 581
Tracking Calls by Account Code 582
Forcing Users to Enter Account Codes 583
Receiving Call-Charge Information 584
Viewing Call Charge Information 587
Setting up Survivable CDR 588

Chapter 18: Administering LDAP Directory Application 595
Overview 595
Configuring the LDAP Directory Service 595
Synchronizing Communication Manager station with the LDAP Directory 596
Configuring the 46xx and 96xx phones 596

Index 597

About this book

Overview

Avaya Aura™ Communication Manager is the centerpiece of Avaya applications. Running on a variety of Avaya S8XXX Servers and DEFINITY 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
  - DEFINITY servers
  - S8100, S8300, S8400, S8500, or S8700-Series Server
- Avaya S8XXX Servers configured as a Local Survivable Processor (LSP).
- Avaya media gateways
  - MCC1 or SCC1 Media Gateways
  - G250, G350, G600, G650, or G700 Media Gateways

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

Intended audience

This document is intended for system administrators and managers, for users interested in information about specific features, and Avaya personnel responsible for planning, designing, configuring, selling, and supporting the system.

Contents

This document includes the following chapters:

- Chapter 1: System Basics tells you how to log in and log off, set permissions for others who use the administration terminal, set daylight savings rules, set the system date and time, post messages, and back up the information you administer.
- Chapter 2: Planning the System provides information on system-wide functions. It explains how to read, use, and make simple changes to your dial plan, and how to assign feature access codes.
- Chapter 3: Managing Telephones explains how to add, swap, and remove telephones, and how to customize a telephone, for Communication Manager administrators.
- Chapter 4: Managing Telephone Features explains how to administer feature buttons for your users' telephones.
- Chapter 5: Managing Attendant Consoles explains attendant console feature buttons, and tells you how to change, move, or add attendant consoles.
- Chapter 6: Managing Displays provides information on the messages that appear on the read-out screen on display telephones.
- Chapter 7: Handling Incoming Calls shows you how to set up call coverage for incoming calls to be sure that incoming calls are answered when the called party is unavailable.
- Chapter 8: Routing Outgoing Calls explains how Avaya Aura™ Communication Manager handles outgoing calls and tells you how to modify call restrictions and your routing plan.
- Chapter 9: Managing Multimedia Calling describes the Multimedia Applications Server Interface (MASI), and provides instructions on administration, monitoring, and troubleshooting. This section also provides information on Multimedia Call Handling (MMCH), which enables users to control voice, video, and data transmissions using a telephone and PC.
- Chapter 10: Setting Up Telecommuting provides information on system-wide settings and individual user administration for telecommuting.
- Chapter 11: Enhancing System Security provides information on analyzing and setting up basic system security, preventing toll fraud, using logins and permissions and passwords, and dealing with security violations.

- Chapter 12: Managing Trunks contains procedures for working with analog and digital trunks. Specialized trunks such as APLT, tandem, release-link, DMI-BOS and ISDN trunk groups are not covered in this manual.
- Chapter 13: Managing Announcements tells you how to record, save, copy, restore and delete announcements.
- Chapter 14: Managing Group Communications shows you how to administer your system so users can page other users or use their telephones as intercoms. You can also give specific users permission to monitor other users' calls or to interrupt active calls with important messages.
- Chapter 15: Managing Data Calls describes the system features available to enable data communications.
- Chapter 16: Administering Avaya Servers describes how to administer an Avaya S8700-Series Server and an Avaya G700 Media Gateway and the Avaya S8300 Server.
- Chapter 17: Collecting Call Information provides information on account codes, and on tracking and collecting billing information about calls.

Conventions used

Become familiar with the following terms and conventions. They help you use this book with Communication Manager.

- A "screen" is the display of fields and prompts that appear on a terminal monitor.
- We use the term "telephone" in this book. Other Avaya books might refer to telephones as phones, voice terminals, stations, or endpoints.
- Keys and buttons are printed in a bold font: **Key**.
- Titles of screens are printed in an initial capital letter: Screen Name.
- Names of fields are printed in a bold font: **Field Name**.
- Text (other than commands) that you need to type into a field are printed in a bold font: **text**.
- Commands are printed in a bold constant width font: **`command`**.
- Variables are printed in a bold constant width italic font: ***`variable`***.
- We show complete commands in this book, but you can always use an abbreviated version of the command. For example, instead of typing **`list configuration station`**, you can type **`list config sta`**.
- If you need help constructing a command or completing a field, remember to use **Help**.
  - When you press **Help** at any point on the command line, the system displays a list of available commands.

  - When you press **Help** with your cursor in a field on a screen, the system displays a list of valid entries for that field.
- Messages that the system displays are printed in a constant width font: **system message**.
- To move to a certain field on a screen, you can use the **Tab** key, directional arrows, or the **Enter** key on your keyboard.
- If you use terminal emulation software, you need to determine what keys correspond to **Enter**, **Return**, **Cancel**, **Help**, and **Next Page** keys.
- We show commands and screens from the newest release of Communication Manager. If your system has an older version of Communication Manager installed, substitute the appropriate commands for your system and see the manuals you have available.
- The status line or message line can be found near the bottom of your monitor. This is where the system displays messages for you. Check the message line to see how the system responds to your input. Write down the message if you need to call the helpline.
- When a procedure requires you to press **Enter** to save your changes, the screen clears. The cursor returns to the command prompt. The message line shows "**command successfully completed**" to indicate that the system accepted your changes.

Admonishments

Admonishments that might appear in this book have the following meanings:

Note:
Draws attention to information that you must heed.

Tip:
Draws attention to information that you might find helpful.

CAUTION:
Denotes possible harm to software, possible loss of data, or possible service interruptions.

WARNING:
Denotes possible harm to hardware or equipment.

DANGER:
Denotes possible harm or injury to your body.

SECURITY ALERT:
Denotes when system administration might leave your system open to toll fraud.

Trademarks

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya, Inc. All other trademarks are the property of their respective owners.

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 Guide, 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

Using Avaya Enterprise Survivable Servers (ESS), 03-300428

What's New in Avaya Aura™ Communication Manager, SIP Enablement Services, Avaya Servers and Media Gateways for Release 5.2, 03-300682

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

How to obtain Avaya books on the Web

If you have internet access, you can view and download the latest version of Avaya documentation products. To view any book, you must have a copy of Adobe Acrobat Reader.

Note:
If you don’t have Acrobat Reader, you can get a free copy at http://www.adobe.com/reader.

For example, to access an electronic version of this book:

1. Access the Avaya Web site at http://www.avaya.com/support/.
2. In the **Go To:** column, click the **Documentation** link.
3. To find a specific book, type the document number (for example, 03-300509 for this book) in the **Search Avaya** text box. Click **GO**.
4. In the resulting list, locate the latest version of the document, and then click the document title to view the latest version of the book.

How to comment on this book

Avaya welcomes your feedback. Contact us through:

- e-mail: document@avaya.com
- fax: 1-303-538-1741
- Contact your Avaya representative

Mention this document's name and number, *Administering Avaya Aura™ Communication Manager,* 03-300509.

Your comments are of great value and help improve our documentation.

How to get help

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

If you need additional help, the following resources are available. You might need to purchase an extended service agreement to use some of these resources. See your Avaya representative for more information.

Go to the Avaya Web site at http://www.avaya.com/support:

- If you are within the United States, click the **Escalation Management** link. Then click the appropriate link for the type of support you need.
- If you are outside the United States, click the **Escalation Management** link. Then click **International Services**, which includes telephone numbers for the international Centers of Excellence. Or contact your local Avaya authorized dealer for any additional help and questions.

Chapter 1: 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 from a system terminal

This procedure provides instructions for logging in from a system terminal, not a remote terminal.

To log into the system:

1. Enter your login name. Press **Enter**.
2. Enter your password. Press **Enter**.

   For security, your password does not display as you type it.
3. Enter the kind of terminal you have or the type your system emulates. Press **Enter**.

   The Command prompt displays.

Note:
If you enter the wrong terminal type, it can lock up your system. If the system is not responding to keyboard commands, type `newterm`. Press **Enter**. Enter the correct terminal type on the new screen. Press **Enter**. If this does not work, turn the power off only on the terminal and then turn it back on. The terminal reboots and you can log in again.

Logging in for remote administration

To log in for remote administration:

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.

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

     You receive data tone or visually receive answer confirmation.

  b. Transfer the voice call to your data terminal.

The Login prompt displays.

2. Complete the steps for Logging into the System on page 17.

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

See also Chapter 11: Enhancing System Security on page 383. 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 a network PCMCIA card, Avaya Site Administration (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

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

You can access an Avaya S8XXX Server directly by plugging a computer into the services port which defaults to port 2 (Eth1) on the back of the server. You must use a crossover cable with an RJ45 connector on each end. Plug the other end into the network connector (NIC card) on the your computer. You might need a NIC card adapter.

Once connected, you can administer the server using three tools:

- Web interface for server-specific administration.
- ASA for various features of Communication Manager
- An SSH client, like PuTTY, and an IP address of 192.11.13.6.

Web Interface : You can access the server Web interface either by connecting directly to the services port on the Avaya S8XXX Server, or by connecting over the customer network.

Connected to the services port : To use the server Web interface:

1. Open the Microsoft Internet Explorer browser. Microsoft Internet Explorer versions 6.0 and 7.0 are supported.
2. In the **Location/Address** field, type **192.11.13.6**. Press **Enter**.
3. When prompted, log in to administer the Avaya S8XXX Server and the features of Communication Manager.

Connected to the customer network : To use the server Web interface:

1. Open the Microsoft Internet Explorer browser.
2. In the **Location/Address** field, type the active server name or IP address. Press **Enter**.
3. When prompted, log in to administer the Avaya S8XXX Server and the features of 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

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 an IP address of 192.11.13.6.

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. ASA is available in several languages.

The S8300, S8400, or S8700-Series Server can be used to download Avaya Site Administration. A downloadable version of this package can be accessed through the S8300, S8400, or S8700-Series Server Web Interface. This software must be installed on a computer running a compatible Microsoft Windows operating system such as Windows 95, 98, NT 4.0, Millennium Edition, Windows 2000, or Windows XP. Once installed, it can be launched from a desktop icon, from the P330 Device Manager, or through a link in the S8300 Server Web Interface.

Installing Avaya Site Administration

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

Operating systems	Processor/RAM
Windows 2000 Windows XP 2003 (Standard and Enterprise)	Pentium-class 300 MHz/64 MB Pentium-class 300 MHz/64 MB Pentium-class 300 MHz/64 MB
Graphics adapter	SVGA with minimum screen resolution of 800 x 600
Floppy disk drive	3-1/2 in. 1.44-MB floppy disk drive
CD-ROM	CD-ROM drive (required to install ASA from CD)
Available hard disk space	A minimum of 100-MB free hard disk space is required. The requirement for disk space depends on the size and number of configuration data sets.
Printer port	Standard PC or network printer port is required for connecting to a printer to produce station button labels.

Operating systems	Processor/RAM
Network adapter	Required for network access to the S8700-Series Server, CM Messaging, and other network-connected systems.
Free serial ports	One free serial port capable of 9600-bps operation is required for a connection to each serial device (UPS). Avaya recommends that PCs have at least a 16550A UART or 16550A UART simulator (capable of 56 kbps DTE-speed connections). USB and internal modems should emulate this hardware. A second serial port is required for simultaneous connection to CM Messaging through a serial connection.

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

To start ASA:

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.

Adding a Switch Administration Item

To add a switch administration item:

1. Click **File > New > Voice Mail System**.

   The system displays the Add Voice Mail System screen.
2. Enter a name in the **Voice Mail System Name** field.
3. Click **Next**. The connection type dialog box displays.
4. Click the **Network connection** radio button.
5. Click **Next**. The Network Connection dialog box displays.
6. Enter the IP address used to connect to the Avaya S8XXX Server.
7. Click **Next**. The Network Connection/Port Number dialog box displays.
8. In the **TCP/IP Port Number** field, enter port **5023**.
9. Click **Next**. The Network Connection/Timeout Parameters dialog box displays. Leave the default values for the timeout parameters.
10. Click **Next**. The login type dialog box displays.
11. Click the **"I want to login manually each time"** radio button.
12. Click **Next**. The Voice Mail System Summary dialog box displays.
13. Check the information, use the **Back** button to make corrections if necessary, and click the **Test** button to test the connection.
14. When the connection is successfully tested, click **Next** and then **Finish**.

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.

Adding a new voice system

When you initially run ASA, you are prompted to create a new entry for the switch connection if you have not already done so. To set up the desired system, click the **New VOICE SYSTEM** icon (on the left of the toolbar row). Complete the Add Voice System wizard to build the system record. When completed, the record will be available in the **Target System** pull-down list.

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 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 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) on page 391.

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 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

To log into the system with ASG:

1. Enter your login ID. Press **Enter**.

   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. Press **ON**.

   The Access Security Gateway Key displays a challenge prompt.

4. At the challenge prompt on the Access Security Gateway Key, type the challenge number without the "-" character (for example, 5551234) from your screen. Press **ON**.

   The Access Security Gateway Key displays a response number (for example, 999-1234).

5. At the response prompt on your terminal, type the ASG response number without the "-" character (for example, 9991234). 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

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

To use the system default Issue of the Day:

1. Log into the Communication Manager server and at the CLI enter

   cp /etc/issue.avaya /etc/issue

   cp /etc/issue.avaya /etc/issue.net

Setting Issue of the Day and Message of the Day

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/elmodocs2/white_papers/CM_Administrator_Logins.pdf.

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.

Strings not permitted in a Message of the Day (case sensitive)

[513]	Software Version	Login:	incorrect login	SAT cannot be executed on a standby server
513]	Password:	ogin	hallenge	
]	assword	ogin:	SAT	

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.

Instructions

To log off:

1. Type **`logoff`**. 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.

Figure 1: Logoff screen

```
Facility Test Call Administered
Remote Access Administered
Alarm Origination is currently disabled
Active major/minor alarm detected; be sure to resolve it

Proceed with Logoff? [n]
```

2. 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

Communication Manager allow 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).

Instructions

Establishing daylight savings rules

To modify a daylight savings rule:

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

   The system displays the **Daylight Savings Rules screen**.

   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).notepad

   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).

2. 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.

3. 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

To display daylight savings time rules:

1. Type **`display daylight-savings-rules`**. Press **Enter**.

   The system displays the **Daylight Savings Rules screen**. 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.

LINUX is used in:

- Avaya S8XXX Server IP-PNC
- Avaya S8XXX Server Fiber-PNC
- Avaya S8XXX Server

Before you start:

- A standard TCP/IP LAN connection is required to connect to the Internet time servers. If a LAN connection is not available, time sync will be done by setting the platform clock manually through the command line or web interface.
- On the target server running Communication Manager, verify if Daylight Savings Time is on.

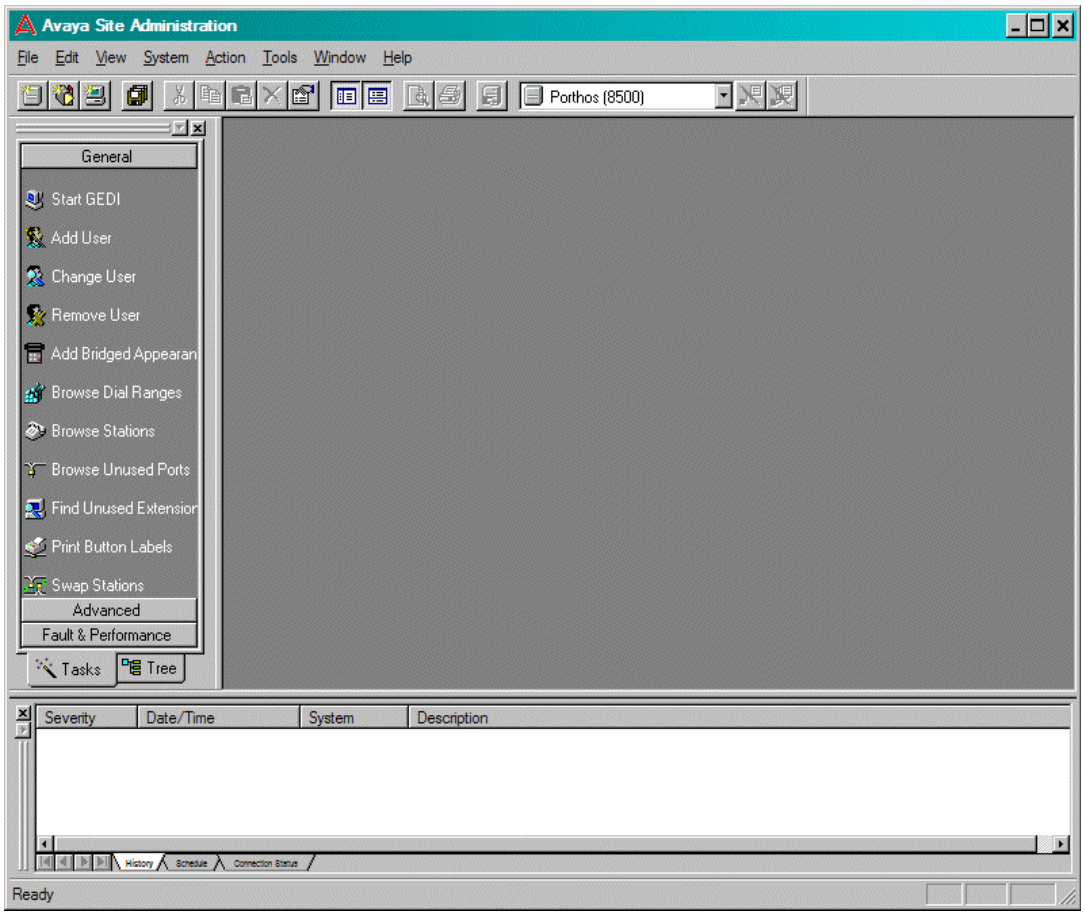
Note:
These instructions are for Avaya DEFINITY CSI servers. For more information, see *Avaya Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568.

To set Time of Day Clock Synchronization:

1. Activate the Avaya Site Administration screen.
2. Click the **Fault & Performance** tab.

   The **Fault & Performance** icons display.

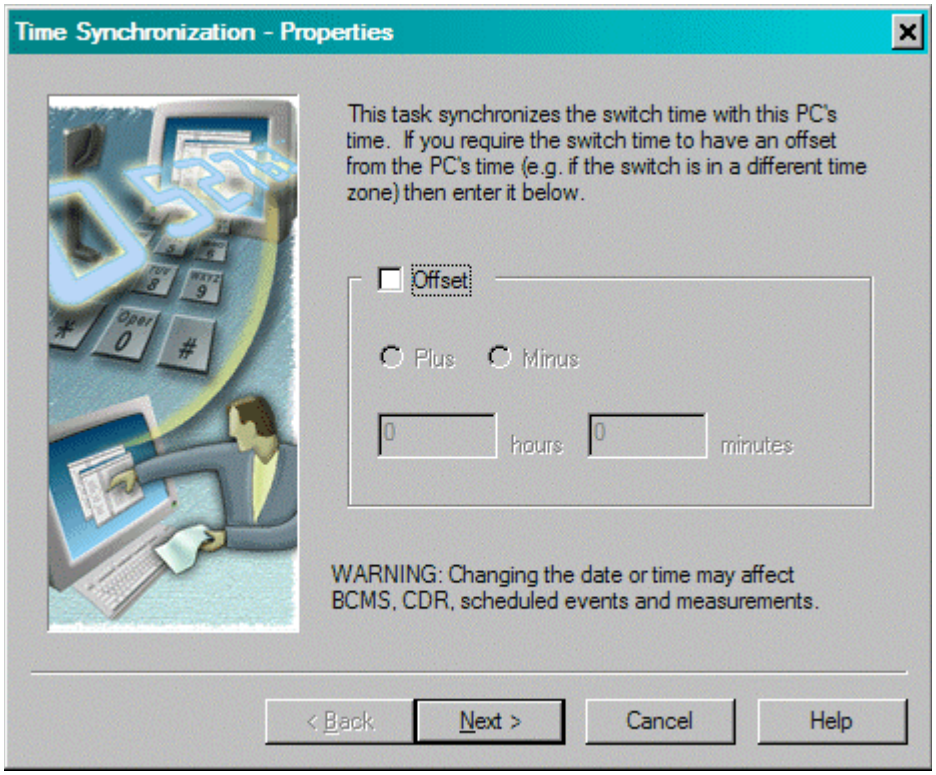
Figure 2: Avaya Site Administration menu



3. Click **Time Synchronization**.

   The Time Synchronization - Properties screen displays.

Figure 3: Time Synchronization - Properties screen



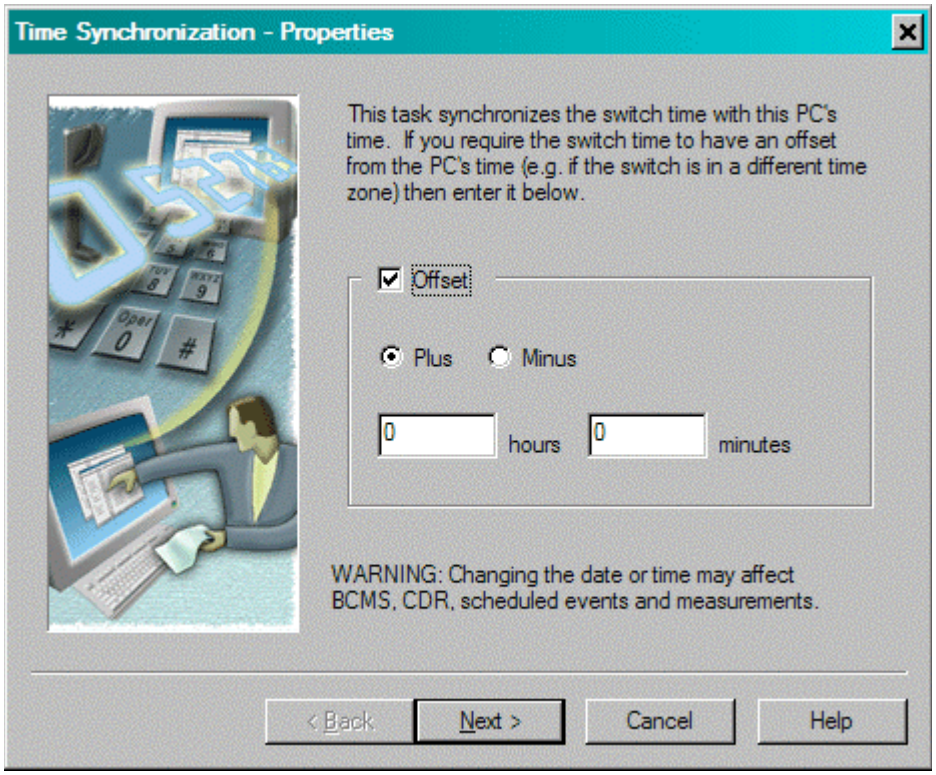
4. Click in the **Offset** box.

   The **Plus** and **Minus** radio buttons and the **Hours and Minutes** fields display.

5. Click **Next**.

   The Time Synchronization - Properties screen displays.

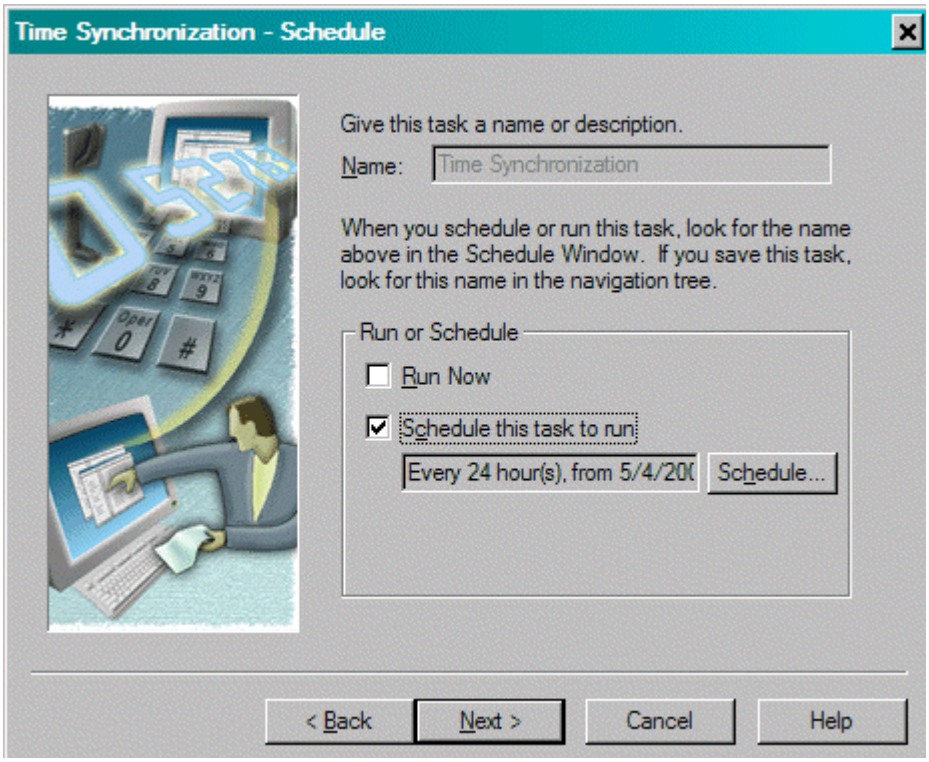
Figure 4: Time Synchronization - Properties screen



6. Click **Plus** to add hours to the remote station (located to the west of the system time) or click Minus to subtract hours to the remote station (located to the east of the system time).
7. In the **hours** field, enter the number of hours to be added or subtracted to synchronize with the remote site.
8. Click **Next**.

   The Time Synchronization - Schedule displays.

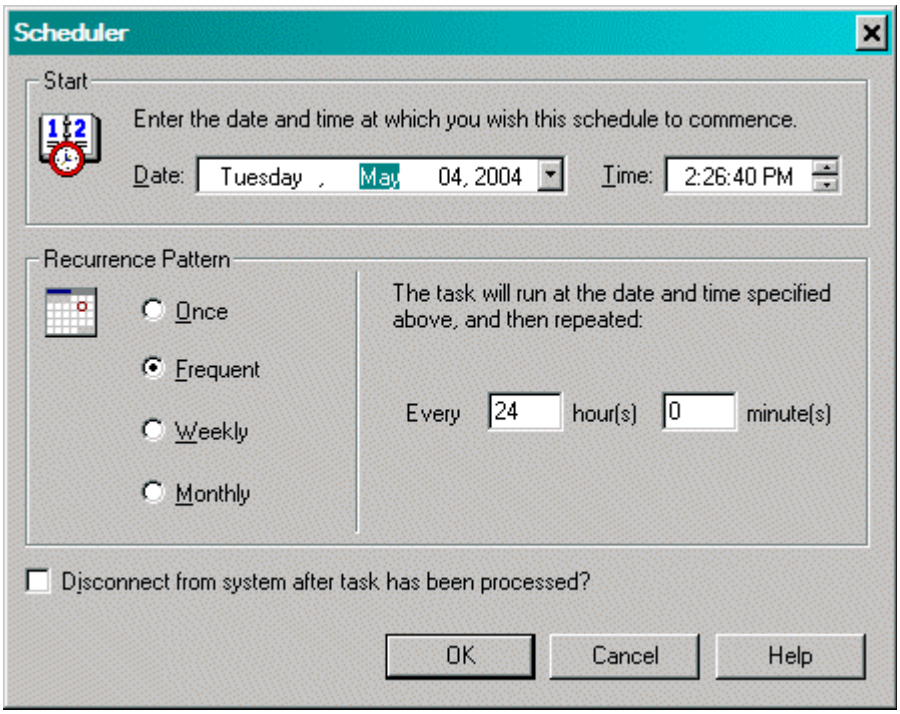
Figure 5: Time Synchronization - Schedule screen



9. Select either:
   - **Run Now** to run this program immediately and click **Next**.
   - **Schedule this task to run** and check the field below to determine if the default setting is satisfactory. If this setting is not satisfactory, click **Schedule**.

   The Scheduler screen displays.

Figure 6: Scheduler screen

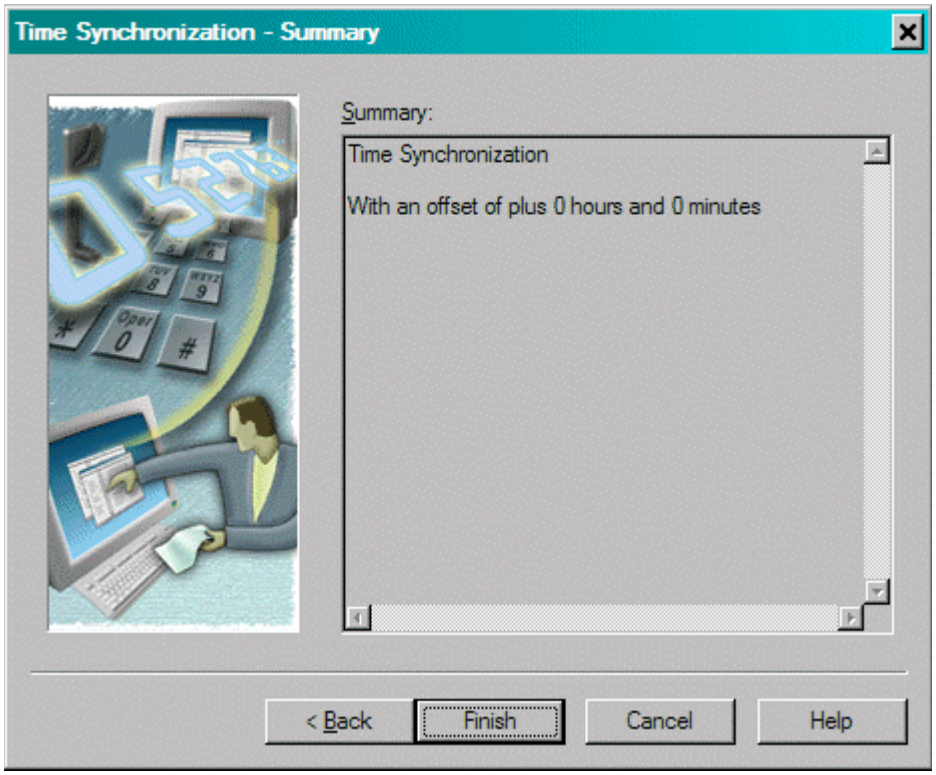


10. In the **Date** field, highlight each object and use the pull-down menu to select the desired setting.
11. In the **Time** field, highlight each item of time and use the pull-down menu to select the desired time.
12. In the **Recurrent Pattern** area, select one radio button for the desired frequency. Notice that each radio button is explained in the area to the immediate right.
13. If there are times to be included, set to the desired frequency.
14. Click **OK**.

    The Time Synchronization - Schedule displays.
15. Click **Next**.

    The Time Synchronization - Summary screen displays.

Figure 7: Time Synchronization - Summary screen



16. If the time synchronization description is satisfactory, click **Finish**.

    If the time synchronization is not satisfactory, click **Back** and revise the necessary information.

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.

For more information about setting time synchronization, see *Avaya Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568.

Setting the System Date and Time

Update the date and time for events such as a leap year, the change to or from daylight savings time, or a system restart after a power failure. The correct date and time assure that Call Detail Recording (CDR) records are correct. CDR does not work until the date and time have been entered.

Note:
Changing the date and time can modify CDR data by 9 hours and 59 minutes. Therefore, you should change the date and time after normal business hours. After you change the date and time, review the time settings for any adjunct (other than CM Messaging) linked to your system that uses the system time.

Before you can set the date and time, you need to know whether it is currently daylight savings or standard time and know which daylight savings rule number you want to use. Daylight savings rule numbers are located on the Daylight Savings Rules screen. For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

In our example, we set the date and time to Tuesday, November 5, 2006 at 8:30 p.m. standard time.

To set the system date and time:

1. Type **set time**. Press **Enter**.

   The system displays the **Date and Time** screen.

2. Complete the **Date** fields.

   a. Type **Tuesday** in the **Day of the Week** field.

   b. Type **November** in the **Month** field.

   c. Type **5** in the **Day of the Month** field.

   d. Type **2006** in the **Year** field.

3. Complete the **Time** fields.

   Use the 24-hour clock to set the hour, so if the current time is 2:00 p.m., you enter **14:00**. You cannot update **Second** — it automatically resets to 0 when you save your changes.

   a. Type **20** in the **Hour** field.

   b. Type **30** in the **Minute** field (8:30 p.m.).

   c. Type **standard** in the **Type** field.

   d. Type **1** in the **Daylight Savings Rule** field.

4. Press **Enter** to save your changes.

   Some display telephones might not automatically refresh the display when you change the date or time. If this occurs, have each user press the date/time button on their telephone to update the display.

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 the system date and time

To display the system date and time:

1. Type **`display time`**. Press **Enter**.

   The system displays the **Date and Time** screen. Verify the information you entered is correct.

Related topics

See Establishing Daylight Savings Rules on page 26 for more information about setting system time.

For additional information, see *Avaya Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568.

Using the Bulletin Board

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 or level 2. If you save translations, the information can be restored if a system reset occurs at levels 3, 4, or 5.

Instructions

Displaying messages

To display the bulletin board:

1. Type **`display bulletin-board`**. Press **Enter**.

   The system displays the Bulletin Board screen.

Posting a message

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.

To post a message to the bulletin board:

1. Type **`change bulletin-board`**. Press **Enter**.

   The system displays the Bulletin Board screen. 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.

2. 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.

3. Press **Enter** to save your changes.

Deleting messages

To delete a message from the bulletin board:

1. Type **`change bulletin-board`**. Press **Enter**.

   The system displays the Bulletin Board screen.

2. Enter a space as the first character on each line of the message you want to delete. Press **Enter**.

3. Press **Enter** to save your changes.

Saving Translations

Communication Manager retains all translation data in memory while the system is operating. If it goes down, you lose all this translation data. You must save in-memory translation data to the memory card (flash ROM), disk, or tape. Saving translation data to memory card or tape is the same as backing up your system.

Note:
Save translations on a daily basis. You might want to save translations after business hours to prevent dial tone delays or during slow business hours if your business is open 24 hours.

The **`save translation`** command writes two time-stamped identical copies of the translation data to the selected memory card, disk, or tape. The save writes one complete copy first, then writes the second copy in a different area of the device — both with the same time-stamp. Failure during a save, including a system crash, usually affects only one copy. The affected copy is marked bad and should not be used for backup.

You can set save translation to be completed automatically as part of regularly scheduled maintenance or manually, as needed. For more information about saving translations automatically, see the maintenance book for your system.

Tip:
To determine if your system saves translations automatically, type **`display system-parameters maintenance`** to see if you have scheduled maintenance.

Translation copy protection assigns a number to a specific telephone system and to the flash card or set of flash cards that belong to that system. For Communication Manager on a DEFINITY Server CSI, this number is the same on both the translation storage device (flash card) and the Flash PROM (Programmable Read Only Memory) of the processor circuit pack. In a duplicated system, the Flash PROM of each processor circuit pack has a translation ID and both ID's are stored on the memory card.

An attempt to initialize (boot) the system with translations that do not contain the same identification number as stored in the processor circuit pack raises a major alarm and disables access to the **`save translations`** command for all non-Avaya logins. You also receive a warning message on the copyright screen notifying you of the mismatch. Contact your Avaya representative to correct this mismatch and reset the **`save translations`** command. You must correct the mismatch before the end of the specified grace period, otherwise you cannot access system management commands (such as: add, change, remove, and duplicate) that modify translation data. Avaya specifies the grace period during a system installation or following an upgrade.

Before you start

If you are saving translations to a memory card or tape, you must verify the memory card or tape is in place and clear any active alarms from the alarms panel.

If you have Communication Manager on a DEFINITY Server CSI, verify the memory card translation ID matches the translation ID of your server's Flash PROM.

Instructions

In our example, we save translations to the tapes on both processor A and B.

To save translations manually:

1. Type **`save translation both tape`**. Press **Enter**.

   The save process can take up to 10 minutes. You cannot administer your system while the save is in process. The Save Translation screen (Figure 8) displays.

Figure 8: Save Translation screen

```
SAVE TRANSLATION


Processor  Command Completion StatusError Code
SPE_A           Success      0
SPE_B           Success      0
```

2. If there is an error message in the **Command Completion Status** field and an error code in the **Error Code** field, clear the error and repeat the save process.

More information

When mass storage system (MSS) devices on both processors in a duplicated server system are specified, translation data is saved from the active processor to the active and standby MSS devices at the same time. If the save to one device fails or one device is out of service, the other save continues. You receive the status of each save separately.

Note:
If you have a duplicated server system and you save translation data to both MSS devices one at a time, translation data inconsistencies between the two devices can occur.

Fixing problems

Note:
You cannot see whether the translation ID on the flash card corresponds to the number on the Processor circuit packs. However, if the numbers do not match, the system issues an error message when you attempt a save translation operation.

When failures occur, the system responds with the following error codes.

Problem	Possible causes	Solution
1	Save translation cannot write to the active drive.	Repeat the save translation process for the active drive.
2	Save translation cannot write to the standby drive.	Repeat the save translation process for the standby drive.

For more information about error messages and how to correct them, or backing up or restoring your system, see the maintenance book for your system.

Performing 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 2: Planning the System

Understanding Your Configuration

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 displays the System Configuration screen, which 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:

- media gateway — the main housing for all the server equipment. Media Gateways are numbered starting with 01.
- carrier — the rack within the media gateway that holds a row of circuit packs. Each carrier within a media gateway 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 media gateway, 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=media gateway, A=carrier, 06=slot, 03=port).

Understanding the Dial Plan

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. The following figure shows an example of a simple dial plan.

Figure 9: Dial Plan Analysis Table screen

```
display dialplan analysis                                          Page 1 of x
                              DIAL PLAN ANALYSIS TABLE
                                 Location: All                  Percent Full: 7

       Dialed  Total  Call        Dialed  Total  Call         Dialed  Total  Call
       String  Length Type        String  Length Type         String  Length Type
         00      2    attd
         1       3    dac
         2       4    ext
         3       5    ext
         3       1    aar
         4       1    ars
         4       5    ext
         5       5    ext
         5       7    ext
         6       5    ext
         7210    7    ext
         8       7    ext
         9       1    fac
         *       3    fac
         #       3    fac
```

The Dial Plan Analysis Table defines the dialing plan for your system.

Note:

In Communication Manager 5.0 and later, you can administer dial plans per-location. Typing the command **`change dialplan analysis`** displays the all-locations Dial Plan Analysis screen. 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.

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. For example, this dial plan shows that when users dial a 5-digit number that starts with 3, they are dialing an extension.

The Dial Plan Analysis Table in our example contains the following call types:

- Attendant (attd) — Defines how users call an attendant. Attendant access numbers can be any number from 0 to 9 and contain 1 or 2 digits.

  In our example figure, the system calls an attendant when users dial 00.

- Dial access code — Allows you to use trunk access codes (TAC) and feature access codes (FAC) in the same range. For example, you could define the group 100 to 199, which would allow both FAC and TAC in that range. Dial access codes can start with any number from 1 to 9, * and #, and contain up to 4 digits.

  In our example figure, dial access codes begin with 1 and must be 3 digits long.

  Note:
  The Dial Plan Analysis Table does not allow you to enter a range specifically for trunk access codes. However, the Trunk Group screen still allows you to assign a TAC to a trunk group. The TAC you enter on the Trunk Group screen must match the format you have administered for a DAC on the Dial Plan Analysis Table.

- Extensions (ext) — Defines extension ranges that can be used on your system. In our figure, extensions must be in the ranges 30000 to 39999, 40000 to 49999 and 50000 to 59999.

- Feature access codes (fac) only — FAC can be any number from 1 to 9 and contain up to 4 digits. You can use * or #, but only as a first digit. In our example, feature access codes can begin with * or # and are 3-digits long.

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.

Displaying your dial plan

You might want to take this opportunity to look at and interpret your own dial plan. To display your system's dial plan:

1. Type **`display dialplan analysis`** or **`display dialplan analysis location`** ***`n`***, where ***`n`*** represents the number of a specific location. Press **Enter**.

Modifying your dial plan

It is easy to make changes to your dial plan. For example, we will add a new range of dial access codes to the dial plan. We want to be able to assign both FAC and TAC in the 700 to 799 range.

1. Type **`change dialplan analysis`** or **`change dialplan analysis location n`**, where ***n*** represents the number of a specific location. Press **Enter**.

   The system displays the Dial Plan Analysis Table screen.
2. Move the cursor to an empty row.
3. Type **7** in the **Dialed String** column. Press **Tab** to move to the next field.
4. Type **3** in the **Total Length** column. Press **Tab** to move to the next field.
5. Type **dac** in the **Call Type** column.
6. Press **Enter** to save your changes.

Adding extension ranges

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. We will add a new set of extensions that start with 3 and are 4 digits long (3000 to 3999).

To add this set of extensions to the dial plan:

1. Type **`change dialplan analysis`** or **`change dialplan analysis location n`**, where ***n*** represents the number of a specific location. Press **Enter**.

   The system displays the Dial Plan Analysis Table screen.
2. Move the cursor to an empty row.
3. Type **3** in the **Dialed String** column. Press **Tab** to move to the next field.
4. Type **4** in the **Total Length** column. Press **Tab** to move to the next field.
5. Type **ext** in the **Call Type** column.
6. Press **Enter** to save your changes.

Administering 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.

Administering a Multi-Location Dial Plan

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.

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 System Parameters Customer-Options (Optional Features) screen. Ensure that the field is set to **y**.

Prepending the location prefix to dialed numbers

Use the **Insert Digits** field on the Uniform Dial Plan Table screen to assign the location prefix from the caller's location on the Locations screen. 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.

- Non-IP telephones and trunks inherit the location number of the hardware they are connected to (for example, the media gateway, 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 media gateway where the C-LAN 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.
- Extension to Cellular endpoints for any applications obtain their location from the Stations with Off-PBX Telephone Integration screen.

For more information about setting up multiple locations, refer to Setting up Multiple Locations on page 256.

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 thee 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.

Adding feature access codes

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 (FAC) 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.

To add a FAC range from 30 to 39:

1. Type **`change dialplan analysis`** or **`change dialplan analysis location n`**, where ***n*** represents the number of a specific location. Press **Enter**.

   The system displays the Dial Plan Analysis Table screen.
2. Move the cursor to an empty row.
3. Type **3** in the **Dialed String** column. Press **Tab** to move to the next field.

4. Type **2** in the **Total Length** column. Press **Tab** to move to the next field.
5. Type **fac** in the **Call Type** column.
6. Press **Enter** to save your changes.

Changing 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. For more information about the dial plan, refer to Understanding the Dial Plan on page 42.

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

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

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

   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 any feature access code, merely delete the existing FAC and leave the field blank.

Administering Dial Plan Transparency (DPT)

The Dial Plan Transparency (DTP) feature preserves users' dialing patterns when a media gateway registers with a local survivable processor (LSP), or when a Port Network requests service from an Enterprise Survivable Server (ESS). Note that this feature does not provide alternate routing for calls made between Port Networks connected via networks other than IP (e.g., ATM or DS1C), and that register to different ESS 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 ESS 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 Port Network	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

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. Refer to Telephone Feature Buttons Table on page 108 for more information.

You can also establish classes of service (COS) to control the Communication Manager features that users can access. For example, you can permit users to forward their calls, or restrict them from placing priority calls. Once you have set permissions for a class of service, you assign this COS to a user's telephone or other device.

Classes of service are very similar to classes of restriction. COR and COS do not overlap in the access or restrictions they control.

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.

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 (Optional Features) screen. For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

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.

This chapter offers a few examples of how you establish these system-wide settings. *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, contains explanations of each of the system parameters screens, and how to use them.

Changing system parameters

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.

To change the number of rings:

1. Type **`change system-parameters coverage/forwarding`**. Press **Enter**.

   The system displays the System-Parameters Call Coverage/Call Forwarding screen.

2. In the **Local Coverage Subsequent Redirection/CFWD No Answer Interval** field, type **2.**
3. 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.

Setting WAN bandwidth limits between network regions

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

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

1. Network topology and WAN link infrastructure.
2. An understanding of the Committed Information Rate (CIR) for the WAN infrastructure.
3. Overlay/design of the Network Regions mapped to the existing topology.
4. Codec sets administered in the system.
5. Bandwidth is assumed to be full duplicated server.

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).

Table 1: Bandwidth usage (in Kbits/sec) based on packet size and codec selection

Packet Size	10 ms	20 ms	30 ms	40 ms	50 ms	60 ms
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.

Instructions

Note:
All DIRECT links must be administered first, and INDIRECT links administered last.

To set bandwidth limitations between directly-connected network regions:

1. Type **`change ip-network region <n>`**, where ***n*** is the region number you want to administer. Press **Enter**.

   The system displays the IP Network Region screen.
2. Scroll to page 3 of the screen, 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.

To set bandwidth limitations between indirectly-connected network regions:

1. Type **`change ip-network region <n>`**, where ***n*** is the region number you want to administer. Press **Enter**.

   The system displays the IP Network Region screen.
2. Scroll to page 3 of the screen, 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 **n**.
5. In the **Intervening-regions** fields, enter up to four intervening region numbers between the two indirectly connected regions.
6. In the **Dynamic CAC Gateway** field, set the gateway that reports the bandwidth limit for this link. The gateway must be configured to be a CAC gateway.
7. Press **Enter** to save your changes.

Note:
Type **`display ip-network region <n>`** to view the current settings of inter-network region connections. Type **`status ip-network region <n>`** to view the current status (that is, bandwidth and number of connections being used) of network-region connections.

Administering Treatment for Denied or Invalid Calls

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

Instructions

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

1. Type `change system-parameters features`. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
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.

Setting up Music-on-Hold

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 *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.

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.

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.

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

To add an audio group:

1. Type **`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. Press **Enter**.

   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

To add a Music-on-Hold group:

1. Type **`add moh-analog-group`** ***`n`***, where ***`n`*** is the Music-on-Hold group number. Press **Enter**.

   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 system parameters for Music-on-Hold

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 that if your system uses Tenant Partitioning, you cannot set up Music on Hold this way. See Providing MOH Service for Multiple Tenants on page 55 for more information.

To set system parameters for MOH:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. In the **Music/Tone On Hold** field, type **music**.

   The system displays the **Type** field.

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**, 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 MOH Service for Multiple Tenants

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.

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

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.

1. Type **`change music-sources`**. Press **Enter**.

   The system displays the **Music Sources** screen.

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. Type `change tenant 1`. Press **Enter**.

   The system displays the Tenant screen.
9. In the **Tenant Description** field, type **Dentist**.

   This identifies the client in this partition.
10. In the **Attendant Group** field, type **1**.

    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, type **change tenant 2**. Press **Enter**.
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.

More MOH information

If a call with either Data Privacy or Data Restriction activated is placed on hold, the Music/Tone on Hold is withheld. This is to prevent transmission of a musical tone that a connected data service might falsely interpret as a data transmission.

If you administer the **Music/Tone on Hold** field to provide music, the system provides the music after a hunt group or Automatic Call Distribution (ACD) split delayed announcement.

Music on Hold might sound distorted when played to IP trunks or to IP telephones through certain codecs, particularly the G.723 codec. You can provide different on-hold materials for these endpoints. Using the instructions for Providing MOH Service for Multiple Tenants, create one tenant partition for all endpoints that do not use the G.723 codec and administer Music on Hold for this tenant. Create another tenant partition for endpoints that use the G.723 codec and administer silence, news, or other material that does not sound distorted for these endpoints.

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.

Before you start

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. For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Make sure that the extensions you notify belong to physical digital display telephones. Refer to Telephone Reference documentation 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.

Instructions

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.

1. Type **`change ars analysis n`**. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen.

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 system displays the Attendant Console screen.

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. See Adding Feature Buttons on page 105 for more information.

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 system displays the Crisis Alert System Parameters screen.

12. Go to the **Every User Responds** field and type **y**.
13. Press **Enter** to save your changes.

More information

Attendants cancel an alert by pressing the crisis alert button three times. The first button push turns off the siren, the second stops the lamp from flashing, and the third clears the display.

Digital telephone users cancel the siren by pushing the crisis alert button. If you have set the system so that only one user needs to respond, this stops the alerting at all telephones. If all users must respond, each telephone continues to alert until that user presses the crisis alert button to acknowledge the alarm. The emergency caller's name and extension remain on the display at this point. To completely cancel an alert and clear their displays, users press the Normal button.

Once you administer Crisis Alert, Communication Manager still records each emergency call and sends a record to the journal printer, if available. If not, you can view the emergency log with the command **`list emergency`**.

Related topics

To determine what types of digital telephones have displays, see the Telephone Reference documentation

For information on setting up Centralized Automatic Message Accounting (CAMA) trunks and providing Caller's Emergency Service Identification (CESID) information to your local community's Enhanced 911 system, see the CAMA Numbering Format screen,

For information about updating station location information without having to change the USA 911 system's Automatic Location Identification database, see the **Emergency Location extension** field in the Station screen.

For information on how to administer IP telephones to make emergency calls, see Setting up emergency calls on IP telephones on page 95.

For more information on individual features, see *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205.

Notifying a Digital Pager of an Emergency

You also 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 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.

Instructions

To set up crisis alert to a digital pager:

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

   The system displays the Crisis Alert System Parameters screen.

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'll 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'll 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.

Related topics

Refer to the Crisis Alert feature in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 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 the Feature-Related System Parameters screen 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 Automatic Callback 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 Temporary Bridged Appearance 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 Distinctive Ringing 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 the Class of Service screen 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

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. For more information on the Station Lock feature, see Station Lock on page 64.

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. For more information about console permissions, see the Class of Service screen.

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.

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

   The system displays the Feature Access Code (FAC) screen.
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 system displays the Feature-Related System Parameters screen. Press **Next Page** to find the **Automatic Exclusion Parameters** section.
6. 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.
7. 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 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 via a FAC. If a digital station has a Station Lock button but activates the feature with the FAC, the LED for the button lights and no special dial tone is provided. However, if a digital station does not have a Station Lock button and activates the feature with the FAC, a special dial tone is provided.

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 T**ime 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
	Assign a Station Security Code (SSC) for a user.	**Security Code**

Screen name	Purpose	Fields
Time of Day Station Lock Table	Administer station lock by time of day.	**Table Active?** **Manual Unlock Allowed?** **Time Intervals**

Chapter 3: 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

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**.

Complete the Station screen for the new telephone and type x in the port field. Note that 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.

Tip:
See Completing the Station screens for more information. See Duplicating telephones if you want to add a number of telephones with similar settings.

Instructions

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:

1. Plug the telephone into the wall jack.
2. Lift the receiver and continue if you hear dial tone.
3. Dial **#****nnnn***, where ***nnnn*** is the extension number of the telephone you are installing.
4. Hang up after you receive confirmation tone.
5. 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.
6. Repeat the process until all new telephones have been installed.
7. 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.
8. Type **n** in the **Customer Telephone Activation (CTA) Enabled** field.
9. Press **Enter** to save your changes.
10. Type **`save translations`**. Press **Enter** to permanently save the changes.
    a. 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:

- find an available port
- wire the port to the cross-connect field or termination closet
- tell the telephone system what you're doing

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.

To add an IP telephone, see Adding an IP telephone on page 92.

Gathering necessary information

Gather the following information:

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. 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.

2. 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.

3. Display the available boards (cards) and ports.

   To view a list of boards on your system, type **`list configuration station`**. Press **Enter**.

   The system displays the System Configuration screen, which 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.

4. 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).

   Tip:
   If you add several telephones at one time, you might want to print a paper copy of the System Configuration screen. To print the screen to a printer attached to the system terminal, type **`list configuration station print`**. Press **Enter**. To print to the system printer that you use for scheduled reports, type **`list configuration station schedule immediate`**. Press **Enter**.

5. 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.

Physically connecting the telephone

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.

Before you start

To download language display labels for telephones, 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, 16xx series telephones, and 96xx series IP Phones 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.

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**.

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**.

Completing the Station screens

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`***

Make sure the extension conforms to your dial plan. You can also use the **`add station next`** command to add a telephone to the **`next`** available extension.

To access the Station screen for the new telephone:

1. Type **`add station`** ***`nnnn`***, where ***`nnnn`*** is the extension for the new telephone. Press **Enter**.

   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 this occurs, try one or more of the following:

   – 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 to **n**.

   – 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.

   When the Station screen appears, you see the extension number and some default field values. For example, the following screen is for a new telephone, displayed by typing **`add station next`**.

2. 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 that the displayed fields might change depending on the model you add.

3. 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`**.

4. 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 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.

   Note:
   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, 16xx series telephones, and 96xx series IP Phones, 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 on page 170. 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.

5. Press **Enter** to save your changes.

To make changes to this new telephone, such as assigning coverage paths or feature buttons, type **`change station`** ***`nnnn`***, where ***`nnnn`*** is the extension of the new telephone. Press **Enter**. See Adding Feature Buttons on page 105 for more information.

Duplicating telephones

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 duplicate the template Station screen to add all the other extensions in the group.

Note that 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.

To duplicate an existing telephone:

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

   Press **Cancel** to return to the command prompt.

2. Type **duplicate station *nnnn*,** where ***nnnn*** is the extension you want to duplicate. 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. If you want to duplicate the station using ***duplicate station <extension> start nnnn count <1-16>,*** you cannot change the station type and the port.

3. 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.

4. Press **Enter** to save your changes to system memory.

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. Press **Enter**

Related topics

You can also add multiple call center agents, all with the same settings based on an agent that is already administered. Enter **`command duplicate agent-loginID`** and the extension of the agent you want to duplicate, then **`start`** and the extension you want to use for the first new agent, then **`count`** and the number of agents you want to add. Fill in the information on the Agent LoginID screen. For more information, see *Avaya Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568.

Using an alias

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.

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`**. Press **Enter**.

   The system displays the **Alias Station** screen.

3. Enter **6220** in the **Alias Set Type** field.

   This is the name or model of the unsupported telephone.

4. Enter **2500** in the **Supported Set Type** field.

   Enter the supported model in this field.

5. Enter **modem** in the second **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.

6. Enter **2500** in the second **Supported Set Type** field.

   Entering 2500 indicates to the system that these models are basic analog devices.

7. Press **Enter** to save your changes.

Now you can follow the instructions for adding a new telephone (or adding a fax or modem). 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 that 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

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.

Tip:
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:

1. Type **`change station 4556`**. Press **Enter**.

   The Station screen for 4556 appears. For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

2. Overwrite **7410+** with **8411D** in the **Type** field.

   Now you can access the functions and feature buttons that correspond to an 8411D telephone.

Swapping telephones

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, and so on.).

For example, to swap telephones for extension 4567 (port 01C0505) and extension 4575 (port 01C0516), complete the following steps:

1. Type **`change station 4567`**. Press **Enter**.
2. Record the current port address (`01C0505`) and type **x** in the **Port** field.
3. Press **Enter** to save your changes.
4. Type **`change station 4575`**. Press **Enter**.
5. Record the current port address (`01C0516`).
6. Type **01C0505** in the **Port** field.
7. Update the **Room** and **Jack** fields.
8. Press **Enter** to save your changes.
9. Type **`change station 4567`** again. Press **Enter**.
10. Type **01C0516** in the **Port** field.

    This is the port that used to be assigned to extension 4575.
11. Update the **Room** and **Jack** fields.
12. Press **Enter** to save your changes.
13. 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.

Using ACTR to move telephones

Automatic Customer Telephone Rearrangement (ACTR) allows a telephone to be unplugged from one location and moved to a new location without additional administration in 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 data base must be manually updated. If the Emergency Location Extension field is not changed or if the USA Automatic Location Identification data base is not updated, the DID number sent to the Public Safety Access Point (PSAP) could send emergency response personnel to the wrong location.

Detailed description

On the Feature-Related System Parameters screen, set the **Terminal Translation Initialization (TTI) Enabled** field to **y** 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.

Call processing

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

Design considerations

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.

Administration

Before you start:

- 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.

Moving telephones

You can allow a telephone to be unplugged from one location and moved to a new location without additional administration on Communication Manager.

For example, to allow moves anytime for a telephone at extension 1234:

1. Type **`change station 1234`**. Press **Enter**.
2. Move to the **Automatic Moves** field.
3. Type **always** in the **Automatic Moves** field.
4. Press **Enter** to save your changes.

Using TTI to move telephones

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 on page 365 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.

Before you start

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.

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 data base must be manually updated. If the **Emergency Location Extension** field is not changed or if the USA Automatic Location Identification data base 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.

Instructions

Merging an extension with a TTI telephone

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

To merge an extension to a telephone with TTI, complete the following steps from the telephone you want to merge:

1. Dial the TTI merge FAC.
   - If the code is correct, you receive dial tone.
   - If the code is not correct, you receive intercept tone.
2. Dial the TTI security code from the telephone you want to merge.
   - If the code is correct, you receive dial tone.
   - If the code is not correct, you receive 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 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 reorder tone. Try the merge again later.
   - If the extension is invalid, you receive intercept tone.
   - If the system is busy and cannot complete the merge, you receive reorder tone. Try the merge again later.
   - If the telephone has a download status of pending, you receive reorder tone. You need to change the download status to complete to successfully complete the TTI merge.

Separating TTI from a telephone

To complete a TTI separation, complete the following steps from the telephone that needs to be separated:

1. Dial the TTI separate FAC.
2. Dial the TTI security code.
   - If the code is correct, you receive dial tone.
   - If the code is not correct, you receive 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 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 intercept tone.
   - If the system is busy and cannot complete the separation, you receive reorder tone. Try the separation again later.

Fixing problems

If you are having difficulty using TTI, you might want to review the following system restrictions:

- 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, the following 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.

- 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 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:

1. Type **`status station 1234`**. Press **Enter**.

   The General Status screen appears.
2. Make sure that the telephone:
   - is plugged into the jack
   - is idle (not making or receiving calls)
   - has no messages waiting
   - has no active buttons (such as Send All Calls or Call Forwarding)
3. Type **`list groups-of-extension 1234`**. Press **Enter**.

   The Extension Group Membership screen shows whether the extension is a member of any groups on the system.
4. Press **Cancel**.
5. If the extension belongs to a group, access the group screen and delete the extension from that group.

   For example, if extension 1234 belongs to pickup group 2, type **`change pickup group 2`** and delete the extension from the list.
6. Type **`list usage extension 1234`**. Press **Enter**.

   The Usage screen shows where the extension is used in the system.
7. Press **Cancel**.

8. If the extension appears on the Usage screen, access the appropriate feature screen and delete the extension.

   For example, if extension 1234 is bridged onto extension 1235, type **`change station 1235`** and remove the appearances of 1234.

9. Type **`change station 1234`**. Press **Enter**.
10. Delete any bridged appearances or personal abbreviated dialing entries. Press **Enter**.
11. Type **`remove station 1234`**. 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.

12. If this is the correct telephone, press **Enter**.

    If the system responds with an error message, the telephone is busy or still belongs to a group. Press **Cancel** to stop the request, correct the problem, and enter **`remove station 1234`** again.

13. Remove the extension from voice mail service if the extension has a voice mailbox.
14. Type **`save translations`**. Press **Enter** to save your changes.

Note that 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 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 modem

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 new telephones on page 70.

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 an alias on page 76.

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.

To add a fax machine as extension 444, complete the following steps:

1. Type **`add station 4444`**. Press **Enter**.
2. In the **Type** field, type **fax**.
3. In the **Port** field, type the port address.
4. In the **Name** field, type a name to associate with this fax.
5. 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.
6. 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.
7. Press **Enter** to save your changes.

Enabling transmission over IP networks for modem, TTY, and fax calls

Prerequisites

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.

To enable transmission over IP networks for modem, TTY, and fax calls:

1. Type **`change ip-codec-set 1`**. Press **Enter**.

   The IP Codec Set screen appears.

Complete the fields as required for each media type you want to enable. Press **Enter**.

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

Adding an H.323 Softphone

Avaya IP (h.323) 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 Communication Manager and then make and receive telephone calls from the telephone extension.

Avaya IP Softphone 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 can 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 road-warrior and the telecommuter configurations for the IP Softphone. Native H.323 registrations for R1 and R2 Softphones continue to be supported.

Before you start

Be sure that your system has been enabled to use IP Softphones. 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

Be sure that your DEFINITY CSI has a C-LAN board and an IP Media Processor board.

Once you're finished administering Communication Manager, you need to install the IP Softphone software on each user's PC.

Adding a single-connect H.323 softphone

You can use the road-warrior mode when you have only a single telephone line available to access 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**.

Except for single-connect IP telephones, you have to administer two extensions for each softphone that will be used in road-warrior mode.

Here is a single-connect example. To use extension 3001 with a softphone in road-warrior mode, you need to administer the telephone (for example, DCP) extension. To do so, complete the following steps:

1. Type **`add station 3001`**. Press **Enter**.

   The system displays the **Station** screen.

   Note that you choose to change an existing DCP extension by using **`change station`** ***`nnnn`*** in this step, where ***`nnnn`*** is the existing DCP extension.

2. In the **Type** field, enter the model of telephone you want to use, such as **6408D**.
3. 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`**.

4. In the **Security Code** field, enter the password for this remote user, such as **1234321**.

   This password can be 3-8 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 your PC. In this example, you can login by entering the DCP extension (3001) and password (1234321).

Adding a softphone to be used in telecommuter mode

Assign this configuration to remote users who have two available telephone lines. For example, to administer a telecommuter mode softphone for a home user at extension 3010, complete the following steps:

1. Type **`add station 3010`**. Press **Enter.**

   The system displays the Station screen.

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 2 and 3.)

2. In the **Port** field, type **x** for virtual telephone or enter the port number if there is hardware.
3. In the **Security Code** field, enter the password for this remote user, such as **1234321**.

   This password can be up to 7 digits in length.
4. In the **IP Softphone** field, type **y**.
5. 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.
6. In the **Multimedia Mode** field, type **enhanced**.
7. Press **Enter** to save your work.

Now you can install and configure the software on your PC. In this example, you can login by entering the DCP extension (3010) and password (1234321).

Fixing problems

Problem	Possible causes	Solutions
Display characters on the telephone can not be recognized.	Microsoft Windows is not set to use Eurofont characters.	Set the Microsoft Windows operating system to use Eurofont.

Related topics

See the online help for assistance, or, on the Avaya IP Softphone CD, refer to *Avaya IP Softphone Overview and Troubleshooting* for customer information on Avaya IP Softphone modes. This is a Portable Document Format (PDF) document that is located in the Overview Document folder on the Avaya IP Softphone CD.

Also see *Getting Started*, also located on the Avaya IP Softphone CD for more information on how to install and configure the IP Softphone software.

Adding an IP telephone

The 4600-series IP Telephones are physical sets that connect to 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.

Before you start

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

Instructions

Let us add an IP telephone at extension 4005.

To assign an extension, complete the following steps:

1. Type `add station 4005`. Press **Enter.**

   The system displays the **Station** screen.

2. In the **Type** field, enter the station type, in this case **4620**.

   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.

3. The **Port** field is display-only, and **IP** appears.
4. In the **Security Code** field, enter a password for the IP telephone user.

   Note:
   Although the system accepts a null password, the IP telephone will not work unless you assign a password.

5. Press **Enter** to save your work.

Changing from dual-connect to single-connect IP telephones

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:

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 system displays the Station screen.

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 changes.

Now 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:

1. Type **`status station 1234`**. Press **Enter**.

   The system displays the General Status screen.

2. Make sure that the extension:
   - is idle (not making or receiving calls)
   - has no messages waiting

- has no active buttons (such as Send All Calls or Call Forwarding)

3. Type **`list groups-of-extension 1234`**. Press **Enter**.

   The Extension Group Membership screen shows whether the extension is a member of any groups on the system.

4. Press **Cancel**.
5. If the extension belongs to a group, access the group screen and delete the extension from that group.

   For example, if extension 1234 belongs to pickup group 2, type **`change pickup group 2`** and delete the extension from the list.

6. Type **`list usage extension 1234`**. Press **Enter**.

   The Usage screen shows where the extension is used in the system.

7. Press **Cancel**.
8. If the 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.

9. Type **`change station 1234`**. Press **Enter**.
10. Delete any bridged appearances or personal abbreviated dialing entries. Press **Enter**.
11. Type **`remove station 1234`**. Press **Enter**.

    The system displays the Station screen for this telephone so you can verify that you are removing the correct telephone.

12. If this is the correct telephone, press **Enter**.

    The system responds with the message `command successfully completed`.

    If the system responds with an error message, the telephone is busy or still belongs to a group. Press **Cancel** to stop the request, correct the problem, and type **`remove station 1234`** again.

13. Remove the extension from voice mail service if the extension has a voice mailbox.
14. Type **`save translations`**. Press **Enter** to save your changes.

Note that 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

Set up which "calling number" to send to the public safety access point when an emergency call is placed from an IP telephone.

Instructions

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.

To prevent an emergency call from an IP telephone:

1. Type **`change station nnnn`**, where ***`nnnn`*** is the extension of the telephone you want to modify. Press **Enter**.

   The system displays the Station screen.
2. Click **Next Page** to find the **Remote Softphone Emergency calls** field.
3. Type **block** in the **Remote Softphone Emergency calls** field.
4. 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.

Setting up Remote Office

Avaya Remote Office provides IP processing capabilities to traditional call handling for voice and data between 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.

Before you start

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

Adding Remote Office to Communication Manager

In our example, we'll set up a remote-office location using Avaya R300 Remote Office Communicator hardware in our branch office in Santa Fe. We'll add a new node, and set up the signaling group and trunk group.

Adding a node

Instructions

To add the remote office node to Communication Manager:

1. Type **`change node-names IP`**. Press **Enter**.

   The system displays the IP Node Names screen.
2. In the **Name** field, type in a word to identify the node.

   In our example, type **Remote 6**.
3. In the IP address field, type in the IP address to match the one on the Avaya R300 administration.
4. Press **Enter** to save your changes.
5. Type **`add remote office`** and the number for this remote office. Press **Enter**.

   The system displays the Remote Office screen.

6. 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
7. 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

You can modify an existing trunk group or add a new one. In our example, we'll add trunk group 6. Before you start, perform Setting up a signaling group on page 98.

To set up the trunk group for your remote office:

1. Type `add trunk group 6`.

   The system displays the Trunk Group screen.
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 **IP** (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

Each Remote Office has own listen port and signaling group. Set up a new trunk group, or use an existing trunk group administered for H.323 signaling.

Instructions

Set up the signaling group for remote office:

1. Type **`add signaling-group`** and the number of the group you want to add.

   The system displays the Signaling Group screen.
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 C-LAN that supports the R300.
6. In the **Far-end Node Name** field, identify the node name assigned to the C-LAN 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

Now we will set up a network region and show the connections between regions.

Instructions

Set up network region 1:

1. Type **`add ip-network-region 1`**. Press **Enter**.

   The system displays the **IP Network Region** screen.
2. In the **Name** field, describe the region you are setting up.
3. In the **Codec Set** field, type the codec set you want to use in this region.
4. In the **UDP Port Range** field, type the range of the UDP port number to be used for audio transport.
5. In the **Intra-region IP-IP Direct Audio** field, type **y**.
6. In the **Inter-region IP-IP Direct Audio** field, type **y**.
7. 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 LSP servers for the network region, and pages 4 through 19 are duplicates of page 3, providing the ability to administer up to 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.

Now you need to assign the region number to the C-LAN circuit pack. All the endpoints registered with a specific C-LAN circuit pack belong to the C-LAN's region. See *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504, for more information.

Adding telephones to Remote Office

Be sure the extensions you add fit your dialing plan.

Instructions

1. Type **`add station nnnn`**, where ***`nnnn`*** is the extension you are adding. Press **Enter**.

   The system displays the Station screen.
2. In the **Type** field, type in the model of the telephone you are adding.
3. In the **Port** field, type **x**.

   This indicates that there is no hardware associated with the port assignment.
4. In the **Name** field, identify the telephone for your records.
5. In the **Security Code** field, match the password set up on the Remote Office administration.
6. In the **Remote Office Phone** field, type **y**.
7. Press **Enter** to save your changes.

Downloading firmware to a 2420 or 2410 DCP telephone

You can copy updated application code into Communication Manager via 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 Communication Manager.

Before you start

1. Type **`change node-name ip`**. Press **Enter**.

   The system displays the IP Node Names screen.
2. Administer the TFTP server node name and the local node name (C-LAN) and IP address.
3. Press **Enter** to save your changes.
4. Type **`change ip-interfaces`**. Press **Enter**.

   The IP Interfaces screen appears.
5. Administer the C-LAN Ethernet interface or processor C-LAN.
6. Press **Enter** to save your changes.

Downloading the firmware file to Communication Manager

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`**. Press **Enter**.

   The system displays the TFTP Server Configuration screen.
7. In the **Local Node Name** field, enter the valid local node name from the IP Node Names screen.

   The node must be assigned to a C-LAN ip-interface or procr (processor C-LAN).
8. In the **TFTP Server Node Name** field, enter the valid TFTP server node name from the IP Nodes Names screen.
9. In the **TFTP Server Port** field, enter the TFTP server port number from where the file download begins.
10. In the **File to Retrieve** field, enter the name of the file to be retrieved.
11. Press **Enter** to save your changes.

    The file transfer begins.
12. Type **`display tftp-server`**. 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.

Downloading firmware to a single station

You must have console permissions to download someone else's telephones.

Note:
Steps 1 through 3 need be done only once to set up the FAC for file downloads. Thereafter, start at step 4 to download files.

To set up a FAC for file downloads:

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

   The system displays the **Feature Access Code (FAC)** screen.
2. Click **Next Page** until you see the **Station Firmware Download Access Code** field.
3. In the **Station Firmware Download Access Code** field, enter a valid FAC as defined in the dial plan.
4. Press **Enter** to save your changes.
5. Take the 2410 or 2420 DCP telephone off-hook.
6. Dial the Station Firmware Download FAC (for instance, *36).
7. Press **#** if you are dialing from the target station (or dial the telephone's extension to be downloaded).
8. 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.
9. When the download completes, the telephone reboots and is released from the busy-out state.

Downloading firmware to multiple stations

You can download firmware to multiple stations of the same type, either 2410 or 2420 DCP telephones. 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 2420 DCP station firmware to multiple stations:

1. Type **`change firmware station-download`**. Press **Enter**.

   The system displays the Firmware Station Download screen.

Figure 10: Firmware Station Download screen

```
 change firmware station-download

                              FIRMWARE STATION DOWNLOAD

Source File:

Schedule Download? y
  Start Date/Time:/: Stop Date/Time:/:
Continue Daily Until Completed? y
Download Set Type: 2420

Beginning Station: Ending Station:
```

2. In the **Source File** field, enter the name of the file specified in the **File to Retrieve** field on the TFTP Server Configuration screen.
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.
9. Press **Enter** to save your changes. 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

You can use the **`status firmware download`** command to display status information for an active download schedule.

1. Type **`status firmware download`**.

2. Press **Enter**.

   The system displays the Status Firmware Station Download screen.

Figure 11: Status Firmware Download screen

```
 status firmware station-download

                              STATUS FIRMWARE STATION DOWNLOAD

Image file:
Schedule Download?               Continue daily until completed?
Start Date/Time:                 Stop Date/Time:

Terminal type for download:
Extension range:     to:         Number of stations in range:
Stations completed:              Stations unsuccessful:
```

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

You can use the **`disable firmware download`** command to disable any active download schedule.

To disable active downloads:

- Type **`disable firmware download`**.

  This command disables any active download schedule and the system displays `Command successfully completed` at the bottom of the screen.

Chapter 4: Managing Telephone Features

Adding Feature Buttons

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 on page 140 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.

To assign feature buttons:

1. Type **`change station`** ***`nnnn`***, where ***`nnnn`*** is the extension for the telephone you want to modify. Press **Enter**.
2. 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.
3. 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 on page 108.

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 on page 106.

4. 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.

Note:
For various features to work properly, a multiappearance station must have a call appearance as the first button. If you try to administer the first button as other than a call-appr (including blank), the station displays the `WARNING: For TTI or PSA to work properly, this button must be a call-appr` warning message on the screen. So, it is a best practice to use the first appearance as a call-appr.

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)

Enabling extended text fields for feature buttons

To enable extended text fields for feature buttons:

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 system displays the Station screen.

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 on page 105.

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 on page 131.

Restricting customization of feature button types

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:

1. Type **`change button-restriction`** and press **Enter**.

   The system displays the **Button Type Customization Restrictions** screen.

2. Ensure that the **Restrict Customization Of Button Types** field 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. 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.

Note:
Starting with Communication Manager Release 5.2, Intuity Audix IA770 application is called Communication Manager Messaging.

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 CM Messaging 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

1 of 24

Table 2: Telephone feature buttons (continued)

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 an abbreviated dialing list entry.	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

2 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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
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

3 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
atd-qcalls	AttQueueCall	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	AttQueueTime	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. A messaging 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-ext
auto-cback	Auto CallBack	Automatic Call Back: when activated, allows inside user who placed a call to a busy or unanswered telephone to be called back automatically when the called telephone becomes available to receive a call.	1 per station
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

4 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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 appearance button the user wants to monitor at this telephone.	Depends on station type
btn-ring	Button Ring	Station User Button Ring Control: allows users to toggle between audible and silent call alerting.	1 per station

5 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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

6 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
call-pkup	Call Pickup	Allows the user to answer a call that is ringing in the user's pickup group.	1 per station
call-timer	Call Timer	Used only with some set 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

7 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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
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	CovrCallBack	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 transmission of the calling-party information over a trunk.	1 per station
cpn-unblk	CPN Unblock	Deactivates the CPN block feature.	1 per station
			8 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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 notification only from callers in the same partition.	1 per station 10 per system
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

9 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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 directory. Note that this is the only way to hide a name in the integrated directory.	1 per station
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

10 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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. • 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.	1 per station

11 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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
extnd-call	Extend Call	Allows the user to extend the current call to an Off-PBX/Extension to Cellular telephone.	1 per station
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
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.	
			12 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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
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
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)

13 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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 media gateways or 1 to 4 for single-carrier media gateway.	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

14 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
man-overid (TOD: _)	ManOverid	Immediate Manual Override (*display button*): allows the user (on a system with Time of Day 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.	1 per station
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. For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878. 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

15 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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
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

16 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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 Mode	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-board alarms (loss of signal, slips, misframes) relate to problems on the facility side of the DS1, ATM, or other interface.	1 per attendant
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

17 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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: • **Ringer On** • **Ringer Off** • **Ringer Delayed** • **Ringer Abbreviated**	1 per station
ringer-off	Ringer Off	Ringer-Cutoff: silences the alerting ringer on the station.	1 per station

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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 system
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
			19 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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 sharing control of the extension. For more information on DMCC, see *Avaya MultiVantage® Application Enablement Services Administration and Maintenance Guide*, 02-300357.	1 per station
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
			20 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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.	up to 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
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 with some set types.	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
			21 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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, you must have both Hospitality and VIP Wakeup enabled.	1 per station
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
			22 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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	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	WhisperAnbk	Whisper Page Answerback: allows a user who received a whisper page to respond to the user who sent the page.	1 per station

23 of 24

Table 2: Telephone feature buttons (continued)

Button name	Button label	Description	Maximum
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
			24 of 24

Adding 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.

Instructions

As an example, we will program a new group list:

1. Type **`add abbreviated-dialing group next`**. Press **Enter**.

   The system displays the Abbreviated Dialing List screen.

2. Enter a number (in multiples of 5) in the **Size** field. This number defines the number of entries on your dialing list.

   For example, if you have 8 telephone numbers you want to store in the list, type **10** in the **Size** field.

3. If you want another user to be able to add numbers to this list, enter their extension in the **Program Ext** field.

   For example, if you want the user at 4567 to be able to change group list 3, enter **4567** in this field.

4. Enter the telephone numbers you want to store, one for each dial code.

   Each telephone number can be up to 24 digits long.

5. 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. For example, we will set up station 4567 so it has access to the new group list.

To give station 4567 access to the group list:

1. Type **`change station 4567`**. Press **Enter**.

   The system displays the Abbreviated Dialing List screen.

2. Press **Next Page** until you see the **Abbreviated Dialing List** fields.

3. Type **group** in any of the **List** fields. Press **Enter**.

   A blank list number field appears.

4. 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.

5. 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.

Fixing problems

Problem	Possible causes	Solutions
A user cannot access a dial list	• The specific list might not be assigned to the user's telephone.	Resolution: 1. Type **`display station nnnn`**, where ***`nnnn`*** is the user's extension. Press **Enter**. 2. 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.
	• If the user attempted to use a feature access code to access the list, they might have dialed the incorrect feature access code.	Resolution: 3. Type **`display feature-access-codes`**. Press **Enter**. 4. Verify that the user is dialing the appropriate feature access code.
	• If the user attempted to press a feature button, they might have pressed the incorrect feature button.	Resolution: 5. Type **`display station nnnn`**, where ***`nnnn`*** is the user's extension. Press **Enter**. 6. Review the current feature button assignments to determine if the user was pressing the assigned button.
		1 of 2

Problem	Possible causes	Solutions
A user cannot access a dial list - *continued*	• If the user attempted to press the correct feature button, the button might not be set up correctly.	Resolution: 1. Type **`display station nnnn`**, where ***`nnnn`*** is the user's extension. Press **Enter**. 2. Review the current feature button assignments to see if the list number and dial code are correct.
A user complains that using an abbreviated dial list dials the wrong number.	• The user could be using the wrong dial code. • The dial code could be defined incorrectly.	Resolution: 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. (For example 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. Correct the number. Press **Enter**.
		2 of 2

More information

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.

Related topics

For more information, see Abbreviated Dialing in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205.

Setting up 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.

Instructions

To create a bridged call appearance:

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.

   For information, see Duplicating telephones on page 75.

3. Type **`change station`** and the bridged-to extension. Press **Enter**.
4. Press **Next Page** until the **Feature Options** page of the Station screen appears.
5. **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**.
6. Move to **Bridge Call Alerting**.

   If you want the bridged appearance to ring when a call arrives at the primary telephone, type **y**. Otherwise, leave the default **n**.

7. Complete the appropriate field for your telephone type.

If. . .	Then. . .
your primary telephone is analog	move to the **Line Appearance** field and enter **abrdg-appr**
your primary telephone is digital	move to the **BUTTON ASSIGNMENTS** field and enter **brdg-appr**

8. 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.

9. 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.

10. Enter the primary telephone extension.
11. 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**.
12. Press **Enter** to save your changes.

To see if an extension has any bridged call appearances assigned, type **`list bridge`** and the extension. Press **Enter**.

More information

Following are 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.

Note:
Best practices for bridged appearances:

- 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.

Setting up 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.

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 external telephone numbers.	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
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 Extension to Cellular use.	Signaling Mode: CAS Interconnect: CO

1 of 2

Table 3: Screens for administering Extension to Cellular (continued)

Screen name	Purpose	Fields
Trunk Group	Administer a trunk group for Extension to Cellular 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 Extension to Cellular. **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 - Extension to Cellular Off-PBX Telephone - OPS Off-PBX Telephone - PBFMC Off-PBX Telephone - PVFMC
		2 of 2

Setting up an Extension to Cellular Feature Access Button

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.

To set up an Extension to Cellular feature button with optional timer:

1. Type **`change station n`** (where ***n*** is the extension of an Extension to Cellular-enabled station - in this example, **`1034`**). Press **Enter**.

2. Press the **Next Page** button till you see the **Button Assignments** fields.
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.

Setting up Terminal Self-Administration

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.

Before you start

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**.

   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.

Instructions

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:

1. Type **`change station 4234`**. Press **Enter**.

   The system displays the Station screen for extension 4234.

2. 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.

3. In one of feature button fields, type **admin**.

   You can assign this button to a feature button or a softkey.

4. Press **Enter** to save your changes.

More information

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.

Fixing problems

- When a telephone is in the Admin mode, the telephone cannot 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 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.
- Since 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.

Setting Up 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 Extension to Cellular 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 that 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 for 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 Enterprise Mobility User

To configure your system for the Enterprise Mobility User feature:

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`**.
4. The system displays the Feature Access Code (FAC) screen. Page down until you see the fields for **Enterprise Mobility User Activation** and **Deactivation**.
5. 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. For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.
7. Click **Enter** to save your changes.

Setting EMU options for stations

To set EMU options for stations:

1. Type **`add station next`**.

   The system displays the Station screen.

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, page 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. Click **Enter** to save your changes.

Defining options for calling party identification

To define the options for calling party identification:

1. Type **`display trunk-group x`**, where ***x*** is the number of the trunk group.

   The system displays the Trunk Group screen.

2. Page 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

Use the following steps to activate a visited telephone:

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 screen 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 T1 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

Use the following steps to deactivate the visited telephone:

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. To deactivate the visited telephone you can:

   – Perform a busy-out, release busy-out at the visited server.
   – Enter the EMU feature deactivation code and the security code of the visited telephone at the home server location.
   – Press the <mute> RESET function on the IP telephone.

Note:
Anytime the visited telephone performs a reset, the EMU registration is deactivated.

– Unplug the visited DCP set for a period of one minute.

Unplugging or disconnecting a 4600 series set will not deactivate the set.

Chapter 5: 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

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. Figure 12 shows the 302A/B console and Figure 13 shows the 302C console. The next two figures show the button layouts on the Feature area and on the optional Selector console.

Figure 12: 302A and 302B1 attendant console

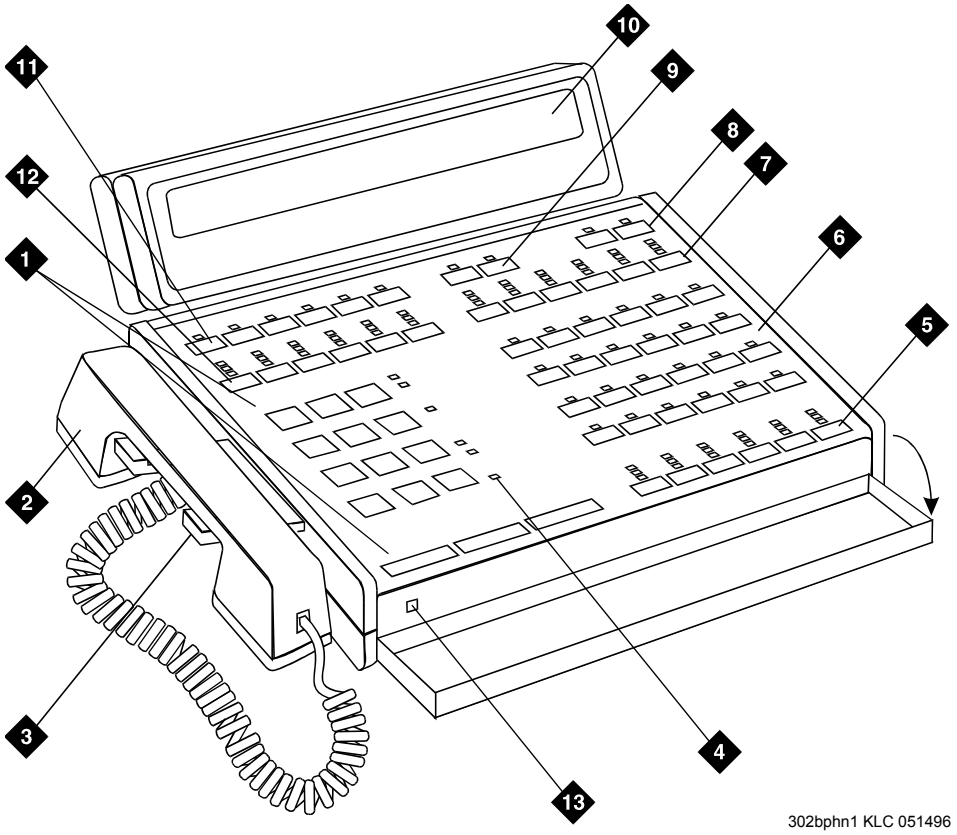


Figure notes:

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

Figure 13: 302C attendant console

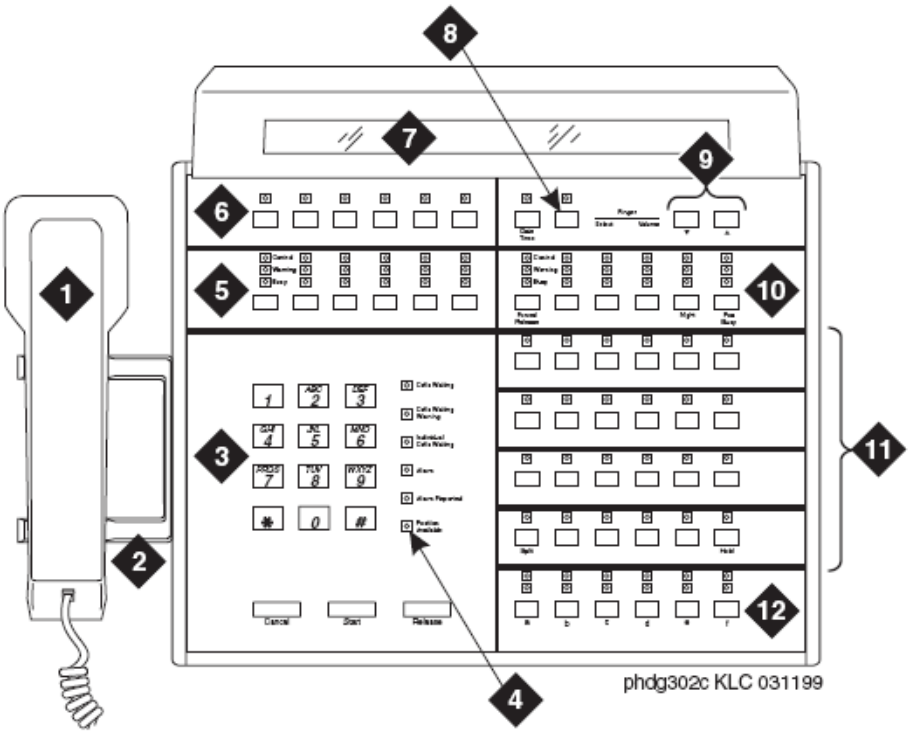


Figure notes:

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

Figure 14: Console feature button layout

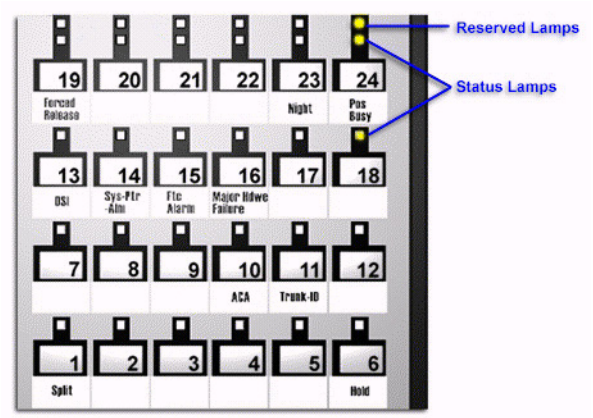
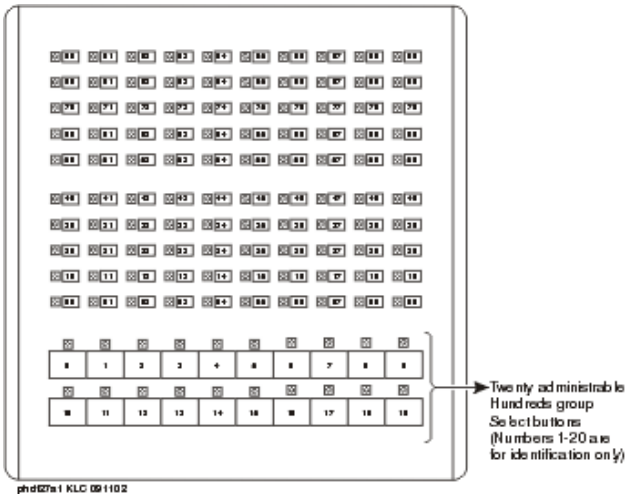


Figure 15: Enhanced Selector Console



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 Communication Manager.

Avaya PC consoles

The Avaya PC Console is a Microsoft Windows-based call handling application for 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.

Adding an Attendant Console

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. Note that these instructions do not apply to adding a PC Console or SoftConsole. For more information, see the appropriate console documentation.

To add a night-only attendant console, complete the following steps:

1. Type **`add attendant`**
2. Press **Enter**.

   The system displays the **Attendant Console Button Layout** screen.
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. Button numbers map to physical positions on the console as shown in Figure 14.

11. Press **Enter** to save your changes.

Attendant Console Feature Buttons

The following table lists the feature buttons that you can assign to an attendant console.

Table 4: Attendant console feature buttons

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
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

1 of 7

Table 4: Attendant console feature buttons (continued)

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
	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
Attendant Room Status	Occupied Rooms Status	occ-rooms	1	6
	Maid Status	maid-stat	1	6

2 of 7

Table 4: Attendant console feature buttons (continued)

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
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	

3 of 7

Table 4: Attendant console feature buttons (continued)

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
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	
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	
				4 of 7

Table 4: Attendant console feature buttons (continued)

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
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 Waiting) [status lamp]	Msg (name or extension #)	aut-msg-wt (Ext:___)	N	
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	

5 of 7

Table 4: Attendant console feature buttons (continued)

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
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	
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

6 of 7

Table 4: Attendant console feature buttons (continued)

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
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	
N = any number of buttons on the telephone can be assigned to this feature. For telephone feature button descriptions, see Telephone Feature Buttons Table on page 108.				
				7 of 7

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 media gateways, 1 to 4 for single-carrier media gateways.
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

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:

1. Type **`change console-parameters`**. Press **Enter**.

   The system displays the **Console Parameters** screen.
2. 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.
3. 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.
4. Press **Enter** to save changes.

Note that some of the settings on the individual Attendant Console screens can override your system-wide settings.

Removing an Attendant Console

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:

1. Type **`status attendant 3`**. Press **Enter**.

   The Attendant Status screen appears.

2. Make sure that the attendant:

   - is plugged into the jack
   - is idle (not making or receiving calls)

3. Type **`list usage extension 4345`**. Press **Enter**.

   The Usage screen shows where the extension is used in the system.

4. Press **Cancel**.

5. 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.

6. Type **`remove attendant 3`**. Press **Enter**.

   The system displays the Attendant Console screen so you can verify that you are removing the correct attendant.

7. 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.

8. Remove the extension from voice mail service if the extension has a voice mailbox.

9. Type **`save translations`**. Press **Enter** to save your changes.

Note that 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

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.*

Before you start

- 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 in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.
- 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) in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Instructions

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.

To configure the system to provide backup alerts and to setup extension 4345 to receive these alerts, complete the following steps:

1. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen.
2. In the **Backup Alerting** field, enter **y**.
3. 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.

4. Type **`change station 4345`**. Press **Enter**.

   The system displays the Station screen.

5. 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.

6. Press **Enter** to save changes.

Now you need to train the user how to interpret the backup alerting and give then the TAAS feature access code so that they can answer the attendant calls.

Return Call to (same) Attendant

Communication Manager Release 5.2 has enhanced the existing attendant features with the Return Call to (same) Attendant feature.

Generally, when an attendant makes a call to a destination that does not answer and has no coverage path, the call returns to the same attendant. If this attendant is busy or unavailable, the call returns to the attendants' group queue.

Communication Manager provides individual queuing functions for each attendant supporting a multiplicity of waiting calls at a given time. When at least one call is waiting in the attendants' group queue the Individual Calls Waiting Indicator is red. Calls are in queue while the attendant is busy.

When you set the **Overflow timer to Group Queue** field on page 2 of the Console Parameters screen to a non-blank value, a call returning to a busy or now unavailable same attendant is placed into an individual waiting queue for this attendant, instead of queuing it into the attendants group. A waiting Return Call moves from the attendant's queue to the attendant group's queue after a certain period of time.

Attendant Timer

Attendant Overflow Timer

Once a call enters the same attendant's queue, the Attendant Overflow Timer starts. When the Attendant Overflow Timer's timer expires, the call moves to the attendants' group queue.

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

Chapter 6: Managing Displays

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

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.

Instructions

We will set up a tie trunk group to receive calling party information and display the calling party number on the telephone of the person called.

1. Type **`change trunk group`** ***`nnnn`***, where ***`nnnn`*** is the trunk group you want to change.

   Press **Next Page** until you see the **Trunk Parameters** fields on the Trunk Group screen (page 2).
2. Type **tone** in the **Incoming Dial Type** field.
3. Press **Next Page** and type ***ANI*DNIS** in the **Incoming Tone (DTMF) ANI** field.
4. Press **Enter** to save your changes.

Displaying ICLID Information

Communication Manager collects the calling party name and number (Incoming Call Line Identification, or ICLID) received from the central office (CO) on analog trunks.

Before you start

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.

Instructions

We will 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.

1. Type **`change trunk group 1`**.

   The system displays the Trunk Group screen for trunk group 1. The **Group Type** field is already set to **diod**.
2. Press **Next Page** to display the Trunk Features fields on the **Trunk Features** screen.
3. Type **Bellcore** in the **Receive Analog Incoming Call ID** field.
4. Press **Next Page** to display the Administrable Timers screen.
5. Type **120** in the **Incoming Seizure (msec)** field.
6. Press **Enter** to save your changes.

Changing the Display Language

This section explains how to set or change the display language.

Setting the display language

To set or change the display language:

1. Type **`change station nnnn`**, where ***`nnnn`*** is the extension of the station that you want to change. Press **Enter**.

   The system displays the Station screen.

Figure 16: Station screen

```
add station next                                          Page 1 of X
                              STATION

Extension:                    Lock Messages? n                       BCC: 0
     Type:                    Security Code:                          TN: 1
     Port:                  Coverage Path 1:                         COR: 1
     Name:                  Coverage Path 2:                         COS: 1
                            Hunt-to Station:

STATION OPTIONS
              Loss Group: 2             Personalized Ringing Pattern: 3
             Data Module? n                       Message Lamp Ext: 1014
            Speakerphone: 2-way                 Mute button enabled? y
        Display Language? English
                   Model:                           Expansion Module?

 Survivable GK Node Name:                          Media Complex Ext:
          Survivable COR:                                IP Softphone? y
   Survivable Trunk Dest?                        Remote Office Phone? y
                                                  IP Video Softphone?
                                                            IP Video?

                                                 Customizable Labels?
```

2. 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 on page 170.

3. Press **Enter** to save your changes.

Entering translations for a user-defined language

WARNING:
Do not use the translation pages if you have installed the file avaya_user-defined.txt.

To enter translations for an existing message using a user-defined language:

1. Type **`change attendant n`**, where ***n*** is the number of the attendant console you want to change. Press **Enter**.

   The system displays the Attendant Console screen.

2. In the **Display Language** field, enter **user-defined**.
3. Press **Enter** to save your changes.
4. Type **`change display-messages n`**, where ***n*** is the message for which you want to translate the display language. Click **help** to view the messages that you can choose to translate. Press **Enter**.

   The system displays the Language Translations screen for the type of message that you want to translate.

5. In the **Translation** field, type the translation of the message in the user-defined language.
6. Press **Enter** to save your changes.

Note:
As of July 1, 2005, new messages are no longer added to the Language Translations screens, so these screens might not show all available Communication Manager messages. The preferred method for entering translations for user-defined telephone messages is to use the *Avaya Message Editing Tool (AMET)*. This tool is available for download from http://support.avaya.com/amet. For more information, see *Avaya Message Editing Tool (AMET) Job Aid*.

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 telephone messages), *custom_unicode.txt* (posted messages and system labels), *avaya_user-defined.txt* (standard telephone messages using Eurofont), and *custom_user-defined.txt* (posted messages and system labels using Eurofont).

To use the Telephone Message files *avaya_unicode.txt* and *custom_unicode.txt*, you must have Unicode-capable stations, such as the 4610SW, 4620SW, 4621SW, and 4622SW, 16xx series telephones, and 96xx series IP Phones, 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 Telephone 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 telephone 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 Telephone Message files

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.

To administer Unicode display:

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 Telephone Message File correctly and such files will fail to install. See the *Avaya Message Editing Tool (AMET) Job Aid* in the Generic Telephone Message Package file for more details on using AMET.
3. Transfer the Telephone 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 Telephone Message files with the Avaya Install Web Page. The Avaya Installation Wizard only supports install of Unicode Telephone Message files. Note that the Installation Wizard is the same wizard that you use to transfer Telephone Message files to an Avaya S8XXX Server that is running Communication Manager 2.2 or later.
5. After you install *avaya_unicode.txt* or *avaya_user-defined.txt*, you must do a reset 4 to load the file in to Communication Manager memory. Note that a reset 4 is *not* required to load the files *custom_unicode.txt* and *custom-defined.txt*.
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 uninstallation option for Telephone Message files. You can reload a new Telephone Message file. This will overwrite existing Telephone Message files.

Checking the status of Telephone Message file loads

To verify that a Unicode Telephone Message file is loaded correctly, run **`status station xxxx`** on any administered station. If the Unicode Telephone 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.

Figure 17: General Status screen

```
 status station nnnn                                          page 2 of x

                                 GENERAL STATUS

CONNECTED STATION INFORMATION
               Part ID Number: unavailable
                Serial Number: unavailable
          Station Lock Active? No

UNICODE DISPLAY INFORMATION
          Native Name Scripts: 0x00000007:Latn;Lat1;LatA
     Display Messages Scripts: 0x04000007:Latn;Lat1;LatA;Jpan
    Station Supported Scripts: 0x7c000007:Latn;Lat1;LatA;Jpan;Chis;Chit;Korn
```

"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 Number	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
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

Script Number	Script Tag Bit (hex)	Start Code.. End Code	Script or Block Name	SAT Screen Name
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 30 31	04000000 08000000 10000000 20000000 40000000	3000..303F	CJKV Symbols and Punctuation	Jpan ChiS ChiT 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

Script Number	Script Tag Bit (hex)	Start Code.. End Code	Script or Block Name	SAT Screen Name
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 30 31	04000000 08000000 10000000 20000000 40000000	FE30..FE4F	CJK Compatibility Forms	Jpan ChiS ChiT Korn Viet

Script Number	Script Tag Bit (hex)	Start Code.. End Code	Script or Block Name	SAT Screen Name
	00000100	FE70..FEFF	Arabic Presentation Forms-B	Arab
26	02000000	FF00..FFEF	Halfwidth and Fullwidth Forms	Kana

Administering displays for QSIG trunks

For proper transmission of QSIG name data for display, administer the following settings:

- Trunk Group screen
  - **Group Type**: **ISDN**
  - **Character Set for QSIG Names**: **iso8859-1**
  - **Outgoing Display**: **y**
  - **Send Calling Number**: **y**
  - **Send Name**: **y**
- Signaling Group screen
  - **Supplementary Service Protocol**: **b**
- System-Parameters Country-Options screen
  - **Display Character Set**: **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 Communication Manager, and therefore cannot be mapped to any other character. An asterisk "*" appears in its place.
	1 of 2

Symptom	Cause and Solution
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.
	2 of 2

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 up Directory Buttons

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.

Instructions

We will 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.

1. Type `change station 2000`. Press **Enter**.

   The system displays the Station screen.
2. Press **Next Page** to move to the **BUTTON ASSIGNMENTS** section.
3. In **Button Assignment** field 6, type **directory**.
4. In **Button Assignment** field 7, type **next**.
5. In **Button Assignment** field 8, type **call-display**.
6. Press **Enter** to save your changes.

Related topics

For more information on LDAP Directory application, see Chapter 18: Administering LDAP Directory Application on page 595.

Making Standard Telephone Features easier to use

Display messages are provided in additional languages for the following standard telephone features:

- Station Security Code
- Personal Station Access
- Call Pickup
- Station Lock

- Extension to Cellular
- Call Forwarding
- Call Coverage
- Call Park

Note:
This feature is applicable only to DCP and IP-H323 terminals, and not to stations that act as attendant consoles. This feature does not support the SIP telephones.

The system administrator can enable or disable the feature in the Feature Related System Parameters screen.

For more information, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878. Following is an example of the display guidance, as shown for Station Security Code. This example is also applicable to features like, Personal Station Access, Call Pickup, Station Lock, Extension to Cellular, Call Forwarding, Call Coverage, and Call Park.

Station Security Code

You can change the Security Code after the system administrator enables the feature on the Feature Access Code (FAC) screen. Use the following change security code procedure for changing the station security code:

End-user administration

Activation

1. After dialing the Feature Access Code (FAC), you can hear a dial tone, and the following text appears:

This text appears together with the dialed digits until the number is complete.

2. After this, you receive no dial tone but the display prompts:

The typed-in security code appears as asterisks (*).

3. Then you receive dial tone and the display prompts:

new security code=

The typed-in security code appears as asterisks (*).

4. Then you receive dial tone and the display prompts:

new security code again=

The typed-in security code appears as asterisks (*).

5. You receive acknowledgement from the confirmation tone (3-beep) and additionally the text appears as follows:

Security code changed

When the call appearance turns to idle (for example, you place the handset on hook, or after timeout) this text is deleted.

Exception handling

The system notifies you with a rejection tone where it detects an incorrect input and the following message displays:

Error!

When the call appearance turns to idle (for example, you place the handset on hook, or after timeout) this text is deleted.

Chapter 7: Handling Incoming Calls

Setting up Basic Call Coverage

This chapter shows you how to set up call coverage for incoming calls to be sure that incoming calls are answered when the called party is not available.

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)

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, CM Messaging, or vector for a station not accepting calls.

Administering system-wide call coverage characteristics

This section shows you how to set up system-wide call coverage characteristics that govern how coverage is handled.

Instructions

The System Parameters Call Coverage/Call Forwarding screen sets up the global parameters which direct Communication Manager how to act in certain situations.

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.

Related topics

For more information on redirecting calls, see Covering calls redirected to an off-site location on page 186.

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

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.

Instructions

To create a coverage path:

1. Type **`add coverage path next`**. Press **Enter**.

   The system displays the Coverage path screen with the next undefined coverage path in the sequence of coverage paths.

2. 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.

3. 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.

4. 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.

5. Press **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

Now assign the new coverage path to a user. For example, we will assign this new coverage path to extension 2054.

Note:
A coverage path can be used for more than one extension.

Instructions

To assign a coverage path:

1. Type **`change station 2054`**. Press **Enter**.

   The system displays the Station screen for extension 2054.

2. 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.

3. Press **Enter** to save your changes.

Related information

Assigning Coverage Options on page 372

Setting up 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

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.

Before you start:

- 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.

To provide coverage of calls redirected to an off-site location:

1. Type **`change system-parameters coverage-forwarding`**. Press **Enter**.
2. The system displays the System-Parameters Coverage-Forwarding screen.
3. Press **Next Page** until you see the **Coverage of Calls Redirected Off-Net (CCRON)** page.

4. In the **Coverage of Calls Redirected Off-Net Enabled** field, type **y**.

   This instructs 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. Press **Enter** to save your changes.

Defining coverage for calls redirected to external numbers

You can administer the system to allow calls in coverage to redirect to off-net (external) or public-network numbers.

Standard remote coverage to an external number allows you 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 not answered 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.

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.

Instructions

For example, to add an external number to coverage path 2:

1. Type **`change coverage remote`**. Press **Enter**.

   The system displays the **Remote Call Coverage Table screen**.

2. 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.

3. Be sure to record the remote code number you use for the external number.

   In this example, the remote code is r01.

4. Press **Enter** to save your changes.
5. Type **`change coverage path 2`**. 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.

6. 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.

7. Press **Enter** to save your changes.

Related topics

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

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.

Instructions

To set up a time-of-day coverage plan that redirects calls for our example above:

1. Type **`add coverage time-of-day next`**. 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.

2. 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.

3. Press **Enter** to save your changes.

Now assign the time-of-day coverage to a user. For example, we use extension 2054:

1. Type **`change station`** ***`nnnn`***, where ***`nnnn`*** is the extension number. Press **Enter**.

   The system displays the **Station** screen.

2. Move your cursors to Coverage Path 1 and type **t** plus the number of the Time of Day Coverage Table.

3. Press **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

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.

Instructions

To add a coverage answer group:

1. Type **`add coverage answer-group next`**. Press **Enter**.

   The system displays the **Coverage Answer Group** screen.

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. Press **Enter** to save your new group list.

   The system automatically completes the **Name** field when you press **Enter**.

Related topics

See Assigning a coverage path to users on page 185 for instructions on assigning a coverage path.

Setting up 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**.

You can also use the Chained Call Forwarding feature to allow calls to be forwarded up to 10 hops (each calling station is considered to be one hop) using a pre-set coverage path within the same switch. For more information, see *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205.

Instructions

To determine which extensions have call forwarding activated:

1. Type **`list call-forwarding`**. 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.

Related topics

See Call Forwarding in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205.

Setting up call forwarding for users

This section shows you how to give your users access to call forwarding.

Instructions

We will change a call forwarding access code from a local telephone with a Class of Service of 1:

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

   The system displays the **Feature Access Code (FAC)** screen.
2. 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.
3. In the **Call Forwarding Activation All** field, type ***71**.

   The ***71** feature access code forwards all calls.
4. In the **Call Forwarding Deactivation** field, type **#72**.

   The **#72** feature access code deactivates the call forwarding option.
5. Press **Enter** to save your changes.
6. Type **`change cos`**. Press **Enter**.

   The system displays the **Class of Service** screen.
7. 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**.
8. 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.

9. 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**.

10. 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.

11. Press **1** to save your changes.

Allowing users to specify a forwarding destination

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.

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

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.

1. They dial their telecommuting extension.

   See Telecommuting Access in *Avaya Aura™ Communication Manager Screen Reference,* 03-602878, for more information. 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 '**#**' key.

   In this example, enter **1014**, then **#**.
4. Even though there is no dial tone, they dial their security code. Press the '**#**' key.

   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

This section shows you how to allow users to change their call coverage path from a local or telecommuting (off-site) telephone.

Instructions

To change call coverage from off-site:

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

   The system displays the Feature Access Code (FAC) screen.
2. 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.
3. Press **Enter** to save your changes.
4. Type **`change cor`**. Press **Enter**.

   The system displays the Class of Restriction screen.
5. In the **Can Change Coverage** field, type **y**.

   This permits users to select one of two previously administered coverage paths.
6. Press **Enter** to save your changes.
7. Type **`change station 1014`**. Press **Enter**.

   The system displays the Station screen for extension 1014.
8. In the **Security Code** field, type **4196**.

   In this example, this is your security code. See the Security-Related System Parameters screen for more information on setting the length of your security code.

9. 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.

10. Press **Enter** to save your changes.

Using 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 telephone, 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 telephone 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.

Activating Enhanced Call Forwarding

To activate Enhanced Call Forwarding using a feature button:

1. Press the feature button labeled **cfwd-enh**

   The telephone 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.

To activate Enhanced Call Forwarding using a feature access code:

1. Press the feature access code for activating Enhanced Call Forwarding.

   The telephone 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

To deactivate Enhanced Call Forwarding using a feature button:

1. Press the feature button labeled **cfwd-enh**

   The telephone 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 to show the status 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.

To deactivate Enhanced Call Forwarding using a feature access code:

1. Press the feature access code for deactivating Enhanced Call Forwarding.

   The telephone 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

To activate or reactivate Enhanced Call Forwarding using a feature button:

1. Press the feature button labeled **cfwd-enh**

   The telephone goes off hook.
2. Press 1 to reactivate Enhanced Call Forwarding
3. Press
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 to show the status 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.

To reactivate Enhanced Call Forwarding using a feature access code:

1. Press the feature access code for activating Enhanced Call Forwarding.

   The telephone 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

To display Enhanced Call Forwarding status using a feature button:

1. Press the feature button labeled **cfwd-enh**

   The telephone goes off hook.
2. Press 3 to display status.

   Your telephone will display the status of the different types of Enhanced Call Forwarding.

To display Enhanced Call Forwarding status using a feature access code:

1. Press the feature access code for displaying Enhanced Call Forwarding status.

   The telephone goes off hook.
2. Press 3 to display status.

   Your telephone will display the status of the different types of Enhanced Call Forwarding.

Activating and deactivating Enhanced Call Forwarding from an off-network telephone

To activate Enhanced Call Forwarding from an off-network telephone:

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.

To deactivate Enhanced Call Forwarding from an off-network telephone:

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.

   You hear a confirmation tone if the activation was successful.

Activating and deactivating Enhanced Call Forwarding from a telephone with console permission

To activate Enhanced Call Forwarding from a telephone with console permission:

1. Press the feature access code for activating Enhanced Call Forwarding.

   The telephone 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 forwarding station extension.
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.

To deactivate Enhanced Call Forwarding from a telephone with console permission:

1. Press the feature access code for activating Enhanced Call Forwarding.

   The telephone goes off hook.

2. Press:
   - 0 for all Enhanced Call Forwarding
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy

Using Enhanced Redirection Notification

In Communication Manager Release 5.2, a visual display or a special dial tone (for a station without display) indicates the activation of redirection features, such as:

- Do Not Disturb
- Send All Calls
- Call Forwarding
- Enhanced Call Forwarding
- Locked Station
- Limit Number of Concurrent Calls
- Posted Messages

For more information, see *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205.

Enabling Enhanced Redirection Notification

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
2. Click **Next** till you see the **REDIRECTION NOTIFICATION** field.
3. Set respective **Display Notification for..?** fields to **y** to enable notification for the required features.
4. In the **Scroll Status messages Timer (sec.)** field, enter a value for the time delay between messages. Leave the field blank to disable scrolling.
5. Press **Enter** to save your changes.

Setting up 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

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.

Instructions

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.

To set up a night station service to voice mail:

1. Type **`add hunt-group next`**. Press **Enter**.

   The system displays the **Hunt Group** screen.

   The **Group Number** field fills automatically with the next hunt group number.

2. 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.

3. Press **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.

4. Type **`change listed-directory-numbers`**. Press **Enter**.

   The system displays the Listed Directory Numbers screen.

5. In the **Night Destination** field, add the night destination on the listed directory telephone.

   In our example, type **51002**.

6. Press **Enter** to save your changes.
7. Type **`change console-parameters`**. Press **Enter**.

   The system displays the **Console Parameters** screen.

8. In the **DID-LDN Only** to **LDN Night Ext** field, type **n**.
9. Press **Enter** to save your changes.
10. 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 CM Messaging.

    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.

11. 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 CM Messaging 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

This section shows you how to set up night console service.

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 205 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.

Instructions

We will put the attendant console (attendant 2) in a night service mode.

To set up Night Console Service:

1. Type **`change attendant 2`**. Press **Enter**.

   The system displays the Attendant Console screen.

2. 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.

3. Press **Enter** to save your changes.

Setting up night station service

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). See Managing Announcements on page 433 for information on setting up the announcement.

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 on page 205.

Instructions

To set up night station service:

1. Type **`change listed-directory-numbers`**. Press **Enter**.

   The system displays the **Listed Directory Number** screen.

2. 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.

3. Press **Enter** to save your changes.

4. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen.

5. In the **DID-LDN Only to LDN Night Extension** field, type **n**.

6. Press **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

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.

To set the feature access code for TAAS:

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

   The system displays the **Feature Access Code (FAC)** screen.

2. Click **Next** until you see the **Trunk Answer Any Station Access Code** field.

3. In the **Trunk Answer Any Station Access Code** field, type **71**.
4. Press **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:

1. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen.
2. In the **EXT Alert Port (TAAS)** field, type **01A0702**.

   Use the port address assigned to the external alerting device.
3. Press **Enter** to save your changes.

Setting up external alerting night service

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.

Instructions

To send LDN calls to the attendant during the day and to a guard's desk at night:

1. Type **`change listed-directory-numbers`**. Press **Enter**.

   The system displays the Listed Directory Numbers screen.
2. In the **Night Destination** field, verify this field is blank.
3. Press **Enter** to save your changes.
4. Type **`change console-parameters`**. Press **Enter**.

   The system displays the **Console Parameters** screen.
5. In the **EXT Alert Port (TAAS)** field, type **01A0702**.

   This is the port address assigned to the external alerting device.

6. Press **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).

To send LDN calls to the attendant during the day and to the TAAS bell at night:

1. Type **`change console-parameters`**. Press **Enter**.

   The system displays the **Console Parameters screen**.

2. 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.

3. In the **Ext Alert Port (TAAS)** field, type **01A070**.

   This is the port address assigned to the external alerting device.

4. Press **Enter** to save your changes.

   The system is in night service.

   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

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.

Instructions

We will direct night calls for trunk group 2 to extension 1245.

To set up trunk group night service:

1. Type **`change trunk-group 2`**. Press **Enter**.

   The system displays the **Trunk Group** screen.

2. 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.

3. Press **Enter** to save your changes.

Setting up night service for hunt groups

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.

Instructions

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.

To administer the hunt group for night service:

1. Type **`change hunt-group 3`**. Press **Enter**.

   The system displays the **Hunt Group screen** for hunt group 3.

2. 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.

3. Press **Enter** to save your changes.

4. Now you need to program a night service button.

   See Adding Feature Buttons on page 105 for more information.

Related topics

See Managing Hunt Groups on page 227.

How do night service types interact?

Here is an example of how several types of night service might be used in one company.

Assume that you already administered the following night service settings:

- Night station night service redirects to extension 3000 and DID-LDN only to LDN Night Ext is set to **n**
- EXT Alert Port (TAAS) field is not defined
- Trunk group 4 redirects to extension 2000

Let us look at how calls for this company are directed after hours:

call type	directs to
An LDN call on a DID trunk	extension 3000
A call on trunk group 4	extension 2000
An internal call to ‘0’	extension 3000
A call that redirects to the attendant through a coverage path	the attendant queue

Adding 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 on page 217, Setting up flexible extended pickup groups on page 220, and Changing extended pickup groups on page 223.

- 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 on page 223.

Throughout this procedure on pickup groups and extended pickup groups, we show examples to make Call Pickup easier to understand.

Call Pickup Alerting

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 on page 213.

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 on page 214, and Assigning a Call Pickup feature access code on page 215.

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 for the duration of the call.
  - 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 while a group member is talking on a pickup call, the member on the pickup call cannot answer the incoming call. If the group member who is already on a pickup call attempts to answer the incoming call to another telephone using Call Pickup, the Call Pickup button status lamp "flutters" for a few seconds. The fluttering status lamp indicates denial of service. The call that the member is currently on is not interrupted.

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:

1. One of the calls to extension A
2. The call to extension B

3. 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.

The following steps are part of the administration process for the Call Pickup feature:

- Administering Call Pickup
  - Setting up Call Pickup
  - Enabling Call Pickup Alerting
  - Assigning a Call Pickup button to a user telephone
  - Assigning a Call Pickup feature access code
- Maintaining Call Pickup
  - Removing a user from a call pickup group
  - Deleting pickup groups
  - Changing a Call Pickup button on a user telephone
  - Removing a Call Pickup button from a user telephone
- Administering Extended Call Pickup
  - Setting up simple extended pickup groups
  - Setting up flexible extended pickup groups
- Maintaining Extended Call Pickup
  - Removing a pickup group from an extended pickup group
  - Changing extended pickup groups
- Administering Directed Call Pickup
  - Setting up Directed Call Pickup
- Maintaining Directed Call Pickup
  - Removing Directed Call Pickup from a user

Setting up Call Pickup

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

To add users to a new call pickup group:

1. Type **`add pickup-group next`**. 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 on page 217. 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 on page 220.

2. Type a name for this pickup group in the **Group Name** field.
3. Type the extension of each group member.

   Up to 50 extensions can belong to one pickup group.

4. Press **Enter** to save your changes.

   The system automatically completes the **Name** field when you press **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

Enabling Call Pickup Alerting

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.

To enable Call Pickup alerting:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
2. Click **Next** until you see the **Call Pickup Alerting** field.
3. Set the **Call Pickup Alerting** field to **y**.
4. Press **Enter** to save your changes.

Enabling Enhanced Call Pickup Alerting

In Communication Manager Release 5.2 and later, Call Pickup Alerting displays calling and called party information. This feature is available to all members of the pickup group and administrable alerting options.

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
2. Click **Next** until you see the **Enhanced Call Pickup Alerting** field.
3. Set **Enhanced Call Pickup Alerting** to **y**.
4. Press **Enter** to save your changes.

Note:
The **Enhanced Call Pickup Delay Timer (sec.) Display** and **Audible Notification** fields are displayed only if **Enhanced Call Pickup Alerting** is set to **y**. To administer the alerting options for a button, you must set the button assignment using the **`change station`** ***n*** command.

Assigning a Call Pickup button to a user telephone

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.

To assign a Call Pickup button for each extension:

1. Type **`change station`** ***n***, where ***n*** is an extension in the pickup group. Press **Enter**.

   The system displays the Station screen.
2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
3. Move to the button number that you want to use for Call Pickup. You can use any of the available buttons.
4. Type **call-pkup** after the button number.

5. Press **Enter** to save your changes.
6. Repeat this procedure for each member of each pickup group.
7. Notify each user what button to use for Call Pickup.

Assigning a Call Pickup feature access code

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.

To create a pickup group feature access code (FAC):

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

   The system displays the Feature Access Code (FAC) screen.
2. In the **Call Pickup Access Code** field, type the desired FAC.

   Make sure that the FAC complies with your dial plan.
3. Press **Enter** to save your changes.
4. Communicate the FAC with each member of each pickup group.

Removing a user from a call pickup group

To remove a user from a pickup group:

1. Type **`change pickup-group`** ***`n`***, where ***`n`*** is the number of the pickup group. Press **Enter**.

   The system displays the Pickup Group screen.
2. Move to the extension that you want to remove.
3. Press **Clear** or **Delete**, depending on your system.
4. Press **Enter** to save your changes.

Deleting pickup groups

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. For more information on extended pickup groups, see Setting up simple extended pickup groups on page 217, and Setting up flexible extended pickup groups on page 220.

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

To get a list of all extended pickup groups:

1. Type **`list extended-pickup-group`**. Press **Enter**.

   The system displays the Extended Pickup Groups screen.
2. Print this screen or write down the existing Group Numbers so that you can check each extended pickup group.
3. Press **Cancel**.

Removing a pickup group from an extended pickup group

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.

To remove a pickup group from an extended pickup group:

1. Type **`change extended-pickup-group n`**, where ***n*** is the extended pickup group that you want to check. Press **Enter**.

   The system displays the Extended Pickup Group screen.
2. Perform one of the following actions:
   - If the pickup group that you want to delete is *not* a member of this extended pickup group, press **Cancel**.
   - If the pickup group that you want to delete is a member of this extended pickup group:
     - Select the pickup group.
     - Press **Clear** or **Delete**, depending on your system.
     - Press **Enter** to save your changes.
3. Repeat this procedure for each extended pickup group.

Deleting a pickup group

To delete a pickup group:

1. Type **`remove pickup-group n`**, where ***n*** is the number of the pickup group that you want to delete. Press **Enter**.

   The system displays the Pickup Group screen.
2. Press **Enter**. The system deletes the pickup group.

Changing a Call Pickup button on a user telephone

To change a call pickup button on a user telephone:

1. Type **`change station n`**, where ***n*** is the extension that you want to change. Press **Enter**.

   The system displays the Station screen.
2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
3. Move to the existing **call-pkup** button.
4. Press **Clear** or **Delete**, depending on your system.
5. Move to the button number that you want to use for call pickup.
6. Type **call-pkup** after the button number.
7. Press **Enter** to save your changes.

Removing a Call Pickup button from a user telephone

To remove a call pickup button from a user telephone:

1. Type **`change station n`**, where ***n*** is the extension that you want to change. Press **Enter**.

   The system displays the Station screen.
2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
3. Move to the existing **call-pkup** button.
4. Press **Clear** or **Delete**, depending on your system.
5. Press **Enter** to save your changes.

Setting up 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.

Creating simple extended pickup groups

To create system-wide simple extended pickup groups:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
2. Click **Next** until you see the **Extended Group Call Pickup** field.
3. In the **Extended Group Call Pickup** field, type **simple**.
4. Press **Enter** to save your changes.

   Your system is now set up for simple extended pickup groups.

Creating an extended pickup group feature access code

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.

To create an extended pickup group feature access code (FAC):

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

   The system displays the Feature Access Code (FAC) screen.
2. Click **Next** until you see the **Extended Group Call Pickup Access Code** field.
3. Perform one of the following actions:
   - If the **Extended Group Call Pickup Access Code** field contains a FAC**,** press **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.
     – Press **Enter** to save your changes.
4. 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. For information on pickup numbers, see Pickup Numbers on page 219.

To create individual pickup groups:

1. If you need to create any pickup groups, see Setting up Call Pickup on page 212.

Assigning pickup groups to a simple extended pickup group

To assign pickup groups to a simple extended pickup group:

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`**. Press **Enter**.

   The system displays the Extended Pickup Group screen for extended pickup group 4.
2. 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).
3. 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.

Setting up 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.

Creating flexible extended pickup groups

To create system-wide flexible extended pickup groups:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
2. Click **Next** until you see the **Extended Group Call Pickup** field.
3. In the **Extended Group Call Pickup** field, type **flexible**.
4. Press **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 on page 218.

To associate individual pickup groups with an extended pickup group:

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`**. 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 on page 223), 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.

2. 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.

As you will see in the Example on page 222, this means that members in pickup group 13 can answer calls to any member that is in extended pickup group 2. The reverse is not true, however. Members that are in extended pickup group 2 cannot answer calls to pickup group 13.

3. Press **Enter** to save your changes.

Assigning pickup groups to a flexible extended pickup group

To assign pickup groups to a flexible extended pickup group:

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 4`**. Press **Enter**.

   The system displays the Extended Pickup Group screen for extended pickup group 4.

2. Add pickup group 16 (Finance) to this extended pickup group. For information how to complete this screen, see Assigning pickup groups to a simple extended pickup group on page 219.
3. Press **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, 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, 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

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.

Changing from simple to flexible

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 on page 221. 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

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 on page 218). After that step, you must re-administer all of the extended pickup groups again.

Setting up 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).

Before you can assign Directed Call Pickup to a user, you must ensure that Directed Call Pickup is available on your system.

To ensure that Directed Call Pickup is enabled on your system:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Directed Call Pickup?** field (see Feature-Related System Parameters screen in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.)

3. Perform one of the following actions:

   - If the **Directed Call Pickup?** field is set to **y**, your system is set up for Directed Call Pickup. Press **Cancel**.
   - If the **Directed Call Pickup?** field is set to **n**:
     - Type **y** in the field.

– Press **Enter** to save your changes.

Creating Classes of Restriction for Directed Call Pickup

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.

To create a COR that allows Directed Call Pickup:

1. Type **`change COR n`**, where ***n*** is the COR that you want to change. Press **Enter**.

   The system displays the Class of Restriction screen (page 1) screen. For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

2. Perform one of the following actions:

   - 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.

   - 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.

   - 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. Press **Enter** to save your changes.

For more information on Class of Restriction (COR), see the "Class of Restriction" feature.

Assigning a Class of Restriction to a user

You must assign a COR to user extensions before anyone can use Directed Call Pickup.

To modify an extension to allow Directed Call Pickup:

1. Type **`change station n`**, where ***n*** is the extension that you want to change. Press **Enter**.

   The system displays the Station screen.

2. In the **COR** field, type the appropriate COR that allows Directed Call Pickup capabilities.
3. Press **Enter** to save your changes.

Assigning a Directed Call Pickup button

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**.

To assign a Directed Call Pickup button for each extension in the COR:

1. Type **`change station n`**, where ***n*** is an extension to which you have assigned the Directed Call Pickup COR. Press **Enter**.

   The system displays the Station screen.

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. Press **Enter** to save your changes.
6. Repeat this procedure for each member of the COR who can pick up other extensions using Directed Call Pickup.
7. Notify each user what button to use for Directed Call Pickup.

Assigning a Directed Call Pickup feature access code

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.

To create a Directed Call Pickup feature access code (FAC):

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

   The system displays the Feature Access Code (FAC) screen.
2. Click **Next** until you see the **Directed Call Pickup Access Code** field.
3. Perform one of the following actions:
   - If the **Directed Call Pickup Access Code** field already contains a code**,** press **Cancel**.
   - 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.
     – Press **Enter** to save your change.
4. 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

To remove Directed Call Pickup from a user:

1. Type **`change station`** ***`n`***, where ***`n`*** is the extension of the user. Press **Enter**.

   The system displays the Station screen.
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. Press **Enter** to save your changes.

Managing Hunt Groups

This section shows you how to set up hunt groups. This section explains how calls to a hunt group are handled, and shows you different call distribution methods.

What are 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

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.

Instructions

To set up our helpline hunt group:

1. Type **`add hunt-group next`**. Press **Enter**.

   The system displays the **Hunt Group screen**. The **Group Number** field is automatically filled in with the next hunt group number.

2. In the **Group Name** field, type the name of the group.

   In our example, type **internal helpline**.

3. In the **Group Extension** field, type the telephone number.

   We'll type **1200**.

4. 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.

5. Press **Next Page** to find the Group Member Assignments screen.
6. 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.

7. Press **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

Related topics

See Hunt Group in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information on an ACD and non-ACD hunt group.

Changing a hunt group

To make changes to a hunt group:

1. Type **`change hunt-group n`**, where ***n*** is the number of the hunt group. Press **Enter**.
2. Change the necessary fields.
3. Press **Enter** to save your changes.

Setting up a queue

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.

Instructions

To set up our helpline queue:

1. Type **`change hunt-group n`**, where ***n*** is the number of the hunt group to change. Press **Enter**.

   In our example, type **`change hunt-group 5`**. The system displays the **Hunt Group screen**.
2. In the **Queue** field, type **y**.
3. In the **Queue Length** field, type the maximum number of calls that you want to wait in the queue.

   In our example, type **10**.
4. 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**.
5. 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**.
6. Press **Enter** to save your changes.

Setting up 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 on page 433). 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

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.

Instructions

To add an announcement to our helpline queue:

1. Type **`change hunt-group n`**. Press **Enter**, where n is the number of the hunt group to change.

   In our example, type **`change hunt-group 5`**.

   The system displays the Hunt Group screen.
2. Press **Next Page** to find the **First Announcement Extension** field.
3. In the **First Announcement Extension** field, type the extension of the announcement you want callers to hear.

   In this example, type **1234**.
4. 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."
5. Press **Enter** to save your changes.

You can use the same announcement for more than one hunt group.

Managing 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 Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 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.

Writing vectors

Writing vectors is easy, but Avaya recommends that you set up and test your vectors before you use them across the system.

We'll write a vector to handle calls to our main number. It is the first vector so we'll use number 1.

Tip:
Use `list vector` to see a list of existing vectors.

Before you start:

- On the System Parameters Customer-Options (Optional Features) screen, ensure that the **Basic Call Vectoring** field is **y**. If not, contact your Avaya representative.
- To provide announcements, you need an Announcement circuit pack. For more information on the circuit pack, see the *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780 and the *Avaya Aura™ Communication Manager Hardware Description and Reference,* 555-245-207.
- Use one of the following:
  - Tone Clock with Call Classifier - Tone Detector circuit pack.
  - Call Classifier - Detector circuit pack.
- Note on adding Meet-Me Conference vectors: If the vector for Meet-Me Conferencing allows a new party to join a conference immediately, and that party is joining as an H.323 ip trunk user, the caller might not have talkpath with the others in the conference. To prevent this, include in the vector a short delay before a new party joins the Meet-Me conference, such as a step to collect digits, a 1-second delay, or play an announcement. Since Meet-Me vectors are always configured with announcements and digit collections, this should rarely be an issue.

To write a vector:

1. Type `change vector 1`. Press **Enter**.

   The system displays the Call Vector screen.

   The vector **Number** field on the left side of the screen is filled in automatically.

2. In the **Name** field, type a description for the vector.

   In our example, type **main number calls**.

   Tip:
   The information in the heading of the Call Vector screen is display only. Use the `display system-parameters customer-options` command to see the features that are turned on for your Communication Manager server.

3. Type your vector steps in the numbered column on the left of the screen.

   Tip:
   When you type in your vector steps, Communication Manager automatically completes some of the vector step information for you. For example, if you type "q" in a vector step field, it fills in "queue-to." Also, additional fields appear when you complete a field. Press **Tab**. This makes it very easy to type in your vector steps.

Now that vector 1 is set up, we will add a vector step to it to tell Communication Manager how to handle the calls to our main number.

Putting a call in a queue

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. See Call Vector screen on page 235.

To queue calls, write the following vector (step 2). (Please note, we started our example on step 2 because step 1 is used later in this chapter.)

Tip:
Remember, Communication Manager automatically fills in some of the information when you type your vector step. Press **Tab**.

Playing an announcement

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 steps 3-5 of the vector, as shown in Call Vector screen.

Routing based on time of day

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):

Figure 18: Call Vector screen

```
change vector 1                                                    page 1 of x
                                CALL VECTOR
   Number:  1       Name: main number calls
              Attendant Vectoring? n     Meet-me Conf? y           Lock? n
     Basic? y  EAS? n   G3V4 Enhanced? y    ANI/II-Digits? y   ASAI Routing? n
 Prompting? y  LAI? n  G3V4 Adv Route? y    CINFO? y   BSR? n      Holidays? n

  01 goto step 7 if time-of-day is all 17:00 to all 8:00
  02 queue-to main split 47 pri 1
  03 announcement 4001 (All agents are busy, please wait...)
  04 wait-time 60 secs hearing music
  05 goto step 2 if unconditionally
  06 stop
  07 disconnect after announcement 4002 ("We're sorry, our office is closed...")
  08 ____________
  09 ____________
  10 ____________
  11 ____________
```

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

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):

Figure 19: Call Vector screen

```
change vector 1                                                    page 1 of x
                                CALL VECTOR
   Number:  1       Name: main number calls
               Attendant Vectoring? n     Meet-me Conf? y           Lock? n
     Basic? y  EAS? n   G3V4 Enhanced? y    ANI/II-Digits? y   ASAI Routing? n
 Prompting? y  LAI? n  G3V4 Adv Route? y    CINFO? y   BSR? n      Holidays? n

  01 goto step 7 if time-of-day is all 17:00 to all 8:00
  02 queue-to main split 47 pri 1
  03 announcement 4001 (All agents are busy, please wait...)
  04 wait-time 60 secs hearing music
  05 goto step 2 if unconditionally
  06 stop
  07 messaging split 99 for extension 2000
  08 _____________
  09 _____________
  10 _____________
  11 _____________
```

Redirecting calls during an emergency or holiday

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:

1. 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.

2. Insert the following bold steps (steps 1, 10, and 11).

   See Inserting a step on page 238 for more information.

Figure 20: Call Vector screen

```
change vector 1                                                    page 1 of x
                                CALL VECTOR
   Number:  1       Name: main number calls
               Attendant Vectoring? n     Meet-me Conf? y           Lock? n
     Basic? y  EAS? n   G3V4 Enhanced? y    ANI/II-Digits? y   ASAI Routing? n
 Prompting? y  LAI? n  G3V4 Adv Route? y    CINFO? y   BSR? n      Holidays? n

  01 goto step 10 if staff agents split 10 > 0
  02 goto step 8 if time-of-day is all 17:00 to all 8:00
  03 queue-to main split 47 pri 1
  04 announcement 4001 (All agents are busy, please wait...)
  05 wait-time 60 secs hearing music
  06 goto step 2 if unconditionally
  07 stop
  08 messaging split 99 for extension 2000
  09 stop
  10 messaging split 99 for extension 2001
  11 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

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:

Figure 21: Call Vector screen

```
change vector 1                                                    page 1 of x
                                CALL VECTOR
   Number:  1       Name: main number calls
               Attendant Vectoring? n     Meet-me Conf? y           Lock? n
     Basic? y  EAS? n   G3V4 Enhanced? y    ANI/II-Digits? y   ASAI Routing? n
 Prompting? y  LAI? n  G3V4 Adv Route? y    CINFO? y   BSR? n      Holidays? n

  01 wait-time 0 seconds hearing music
  02 collect 4 digits after announcement 4004 (You have reached our company.
        Please dial a 4-digit extension or wait for the attendant.)
  03 route-to digits with coverage y
  04 route-to number 0 with cov n if unconditionally
  05 stop
  06 ____________
  07 ____________
  08 ____________
  09 ____________
  10 ____________
  11 ____________
```

Inserting a step

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.

To insert a new vector step in vector 20:

1. Type **`change vector 20`**. Press **Enter**.

   The system displays the Call Vector screen.

2. Press **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. Press **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

To delete vector step 5 from vector 20:

1. Type **`change vector 20`**. Press **Enter**.

   The system displays the Call Vector screen.
2. Press **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**. Press **Enter**.
4. Press **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.

Using 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 Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780.

Administering vector variables

Administering variables and implementing them in your vectors is a relatively simple process:

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`**. Press **Enter**.

   The system displays the **Variables for Vectors** screen.
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. Press **Enter** to save your changes.

Note:
For more detailed descriptions of fields, see the Variables for Vectors screen in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878. For a more detailed description and examples of vectors and vector variables, see *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780.

Handling TTY calls with vectors

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 on page 433.

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:

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.

More information

See the *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 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

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:

1. Type **`display events`**. Press **Enter**.

   The system displays the Event Report screen.

Figure 22: Event Report screen

```
display events                                                    page 1 of x
                                EVENT REPORT
         The following option control which events will be displayed:
            EVENT CATEGORY
                        Category: Vector
            REPORT PERIOD
                        Interval: _a_ From: __/__/__:__ To: __/__/__:__
            SEARCH OPTIONS
                        Vector Number: __
                        Event Type: ___
```

2. To see all current vector events, press **Enter**.

   OR

   Indicate the events that you want to see by completing the **Report Period** and **Search Option** fields. See *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780, for more information.

3. Press **Enter** to view the report.

   The system displays the Event Report (detail) screen.

Figure 23: Event Report screen

```
display events                                                  page 1 of x
                                EVENT REPORT
Event Event                  Event    Event    First        Last         Event
Type  Description             Data 1   Data 2   Occur        Occur        Cnt
  20  Call not queued         12/5     B        09/28/13:43  09/28/13:43  21
 541  Not a messaging split   Split    4C       09/28/13:43  09/28/13:43  136
```

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

Working with 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

To add a vector directory number:

1. Type **`add VDN 5011`**. Press **Enter**.

   You enter the VDN extension you want to add. The system displays the **Vector Directory Number screen**.

2. 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.

3. Enter the vector number.

   In our example, type **11**.

4. 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.

5. Press **Enter** to save your changes.

Viewing vector directory numbers

To see the VDNs already associated with your vectors:

1. Type **`list VDN`**. Press **Enter**.

   The system displays the **Vector Directory Number screen**.

Figure 24: Vector Directory Number screen

```
list vdn
                     VECTOR DIRECTORY NUMBER
                                                                  Event
                                   VDN          Vec        Orig   Notif  Skills
Name                        Ext    Ovrd  COR TN Num  Meas  Annc   Adj 1st 2nd 3rd
Tech Support                5000   y     59  1  234  none  301
Customer Serv.              5001   n     1   1    1  none  302
New Orders                  5002   y     23  1    5  none  303
```

2. Each VDN maps to one vector. Several VDNs can map to the same vector.

Understanding Automatic Call Distribution

Automatic Call Distribution (ACD) is a 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 Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568, for more information on ACD call centers.

Enhancing an ACD system

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 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. See What are vectors? on page 232 for more information.

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. Communication Manager uses these classifications to match each call with the best available agent. See *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780, for more information on call vectoring and EAS.

Assigning a Terminating Extension Group

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.

Instructions

Now assign a terminating extension group to the advertising department. For example, we will assign this TEG to extension 6725.

1. Type **`add term-ext-group next`**. Press **Enter**.

   The system displays the **Terminating Extension Group** screen.

2. In the **Group Extension** field, type **6725**.

   This is the extension for the advertising group.

3. In the **Group Name** field, type **advertising**.

   This is the name of the group.

4. In the **Coverage Path** field, type **5**.

   This is the number of the call coverage path for this group.

Chapter 8: 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. 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.

Managing Calling Privileges

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 (FRL) on the Class of Restriction screen. The FRL determines the calling privileges of the user. Facility Restriction Levels are ranked from 0 to 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.

Instructions

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:

1. Type **`change station 1234`**. Press **Enter**.

   The system displays the Station screen.
2. In the **COR** field, type **7**. Press **Enter** to save your changes.
3. To change from FRL 0 to FRL 7, type **`change cor 7`**. Press **Enter**.

   The system displays the Class of Restriction screen.
4. In the **FRL** field, type **7**. Press **Enter** to save your changes.

Now all users with COR 7 will have the highest level of calling permissions.

Assigning ARS FAC

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.

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. It will not be part of the digit analysis.

Instructions

To assign the ARS FAC:

1. Type **`change dialplan`**. Press **Enter**.

   The system displays the Dial Plan Analysis Table screen.
2. Move to the 9 row and type **fac** in the first column. Press **Enter** to save your changes.
3. Type **`change features`**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen.
4. Type **9** in the **ARS - access code** field.
5. 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 in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878). 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 FAC 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

Instructions

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:

1. Type **`display ars analysis 1`**. Press **Enter**.

   The ARS Digit Analysis Table for dialed strings that begin with 1 appears. Note that 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.

To see all the dialed strings that are defined for your system, run an ARS Digit Analysis report:

1. Type **`list ars analysis`**. Press **Enter**.

The system displays the ARS Digit Analysis Report screen. You might want to print this report to keep in your paper records.

Understanding 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

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.

The table below 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.

Table 5: ARS digit conversion examples

Operation	Actual Digits Dialed	Matching Pattern	Replacement String	Modified Address	Notes
DDD call to ETN	9-1-303-538-1345	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	9-1-201-957-5567 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 intercept treatment	9-1-212-976-1616	1-XXX-976	#	(blank)	"#" means end of dialing. ARS ignores digits dialed after 976. User gets intercept treatment.
International calls to an attendant	9-011-91-672530	011-91	222-0111#	222-0111	Call routes to local server (RNX 222), then to attendant (222-0111).

1 of 2

Table 5: ARS digit conversion examples (continued)

Operation	Actual Digits Dialed	Matching Pattern	Replacement String	Modified Address	Notes
International call to announcement (This method can also be used to block unauthorized IDDD calls)	9-011-91-6725 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.
					2 of 2

Defining operator assisted calls

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.

To see how Communication Manager handles a call to an operator:

1. Type **`display ars analysis 0`**. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen starting with 0. The table shows the translations for calls that begin with 0.

Instructions

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

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.

Instructions

To see how Communication Manager handles a call to an IXC:

1. Type **`display ars analysis 1`**. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen starting with 1.

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.

Restricted area codes and prefixes

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 on page 254 for more information.

Instructions

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.

To deny long distance calls to the 200 area code:

1. Type **`change ars analysis 120`**. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen beginning with 120. The table shows the 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

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.

Instructions

To prevent callers from placing calls to long-distance 555 information numbers:

1. Type **`change ars analysis 1`**. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen beginning with 1.
2. Use the arrow keys to move to a blank **Dialed String** field.
3. Enter **1xxx555** in the **Dialed String** field.
4. Enter **11** in the **Total Min** and **11** in **Total Max** fields.
5. Enter **deny** (denied) in the **Route Pattern** field.

6. Enter **fnhp** in the **Call Type** field.
7. Press **Enter** to save your changes.

Defining local information calls

You can set up Communication Manager to allow calls to local information, or in this example, 411.

Instructions

To allow 411 service calls:

1. Type **`change ars analysis 4`**. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen beginning with 4.
2. Use the arrow keys to move to a blank **Dialed String** field.
3. Enter **411** in the **Dialed String** field.
4. Enter **3** in the **Total Min** and **3** in **Total Max** fields.
5. Enter **1** in the **Route Pattern** field.
6. Enter **svcl** (service call) in the **Call Type** field.
7. Press **Enter** to save your changes.

Administering Call Type Digit Analysis

There must be at least one entry in the Call Type Digit Analysis Table for Call Type Digit Analysis to take place.

1. Enter **`change calltype analysis`**.

   The system displays the Call Type Digit Analysis Table screen.
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.

   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.

```
display calltype analysis                                          Page 1 of x
                         CALL TYPE DIGIT ANALYSIS TABLE
                                     Location:   all
    Dialed String             Delete Insert     Type    Delete Insert       Type
Match: 303_________________ 1: 0      __________ ars  2: 0__    1___________ ars
length: Min 10 Max 10    __ 3: 3      __________ ext  4: 0      011_________ ars
```

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

You can define a location number for:

- Remote Offices
- Media gateways
- IP network regions, used by IP stations and IP trunks
- Extension to Cellular endpoint

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 more information about the location number, refer to Prepending the location prefix to dialed numbers on page 45.

Before you start

Ensure that 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. 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`** commands in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers,* 03-300431.

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

Instructions

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:

1. Type **`change locations`**. Press **Enter**.

   The system displays the **Locations** screen.

2. 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.

3. Type **Chicago** in the **Name** field in the Number **1** row.

   Use this field to identify the location.

4. 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.

5. 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.

6. 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.

7. Type **New York** in the **Name** field in the Number **2** row.
8. 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.

9. 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.

10. 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.

11. Press **Enter** to save your changes.

Related topics

See *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205, for more information on the Multiple Locations feature.

See Setting the System Date and Time on page 34 for more information about how to set your system clock and specify the daylight savings rule for the location.

See Establishing Daylight Savings Rules on page 26 for more information about how to specify the dates and times of daylight savings rules.

Routing with Multiple Locations

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**.

Before you start

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. For information about this screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

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

Instructions

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:

1. Type `change ars analysis location 1`. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen for location 1.

2. 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:

   - Type the appropriate digit in the **Dialed String** field.
   - Type **7** in the **Total Min** field.
   - Type **7** in the **Total Max** field.

- Type **2** in the **Route Pattern** field.
- Type **hnpa** in the **Call Type** field.

In our example, for location 1 (Chicago) local service calls:

- Type the appropriate digits in the **Dialed String** field.
- Type **3** in the **Total Min** field.
- Type **3** in the **Total Max** field.
- Type **1** in the **Route Pattern** field.
- Type **svcl** in the **Call Type** field.

3. Press **Enter** to save your changes.
4. Type `change ars analysis 4 location 2`. Press **Enter**.

   The system displays the ARS Digit Analysis Table for location 2.
5. Type in the local HNPA and service call routing information for New York.
6. Press **Enter** to save your changes.

Related topics

See Automatic Routing in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205, for more information on ARS.

See AAR and ARS Digit Analysis Table, AAR and ARS Digit Conversion Table, and Toll Analysis in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for general information on ARS administration. You can define location specific entries in addition to the global entries on these screens.

See Multiple Locations in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205 for more information on the Multiple Locations feature.

Modifying Call Routing

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

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.

Instructions

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, 3, and 5 in our example. Also, enter **10** in the **Total Min** and **Total Max** fields (instead of 11) in step 6.

To add this non-local area code:

1. Type **`list ars route-chosen 14152223333`**. 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.

Figure 25: ARS Route Chosen Report screen

```
list ars route-chosen 14152223333

                            ARS ROUTE CHOSEN REPORT

     Location: 1                        Partitioned Group Number:  1

      Dialed               Total      Route    Call      Node      Location
      String              Min  Max    Pattern  Type      Number
      141                 11   11     30       fnpa                all
```

2. 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**.

3. Type `change ars analysis 1650`. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen.

4. 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.

5. Enter **1650** in the **Dialed String** field.
6. 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.

7. Enter the route pattern from step 2 in the **Route Pattern** field.

   In our example, enter **30**.

8. Enter **fnpa** in the **Call Type** field.
9. Enter the node number from step 2 in the **Node Num** field.

   For our example, leave the node number blank.

10. 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. See Setting up Multiple Locations on page 256.

Using ARS to restrict outgoing calls

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

Instructions

To prevent callers from placing calls to Colombia (57):

1. Type **`change ars analysis 01157`**. Press **Enter**.

   Enter 011 (international access) and the country code (57). The system displays the ARS Digit Analysis Table screen.
2. 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. Skip to Step 5 to deny calls to this dialed string.
3. Enter **01157** in the **Dialed String** field.
4. Enter **10** in the **Total Min** and **23** in **Total Max** fields.
5. Enter **deny** (denied) in the **Route Pattern** field.
6. Enter **intl** in the **Call Type** field.
7. Press **Enter** to save your changes.

Overriding Call Restrictions

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.

Before you start

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.

Instructions

We will create an authorization code 4395721with a COR of 2.

1. Type **`change authorization-code 4395721`**. Press **Enter**.

   The system displays the Authorization Code - COR Mapping screen.
2. In the **AC** field, type **4395721**.
3. In the **COR** field, enter **2**.
4. Press **Enter** to save your changes.

Defining 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 Communication Manager and you want to continue to use partitioning, please read this section carefully. In this release of 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.

Before you start

- 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**.

Setting up partition groups

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.

Instructions

To enable 1-800 calls for partition group 2:

1. Type **`list ars route-chosen 18002221000`**. Press **Enter.**

   You can use any 7-digit number following the 1800 to create an example of the dialed string.

   The system displays the ARS Route Chosen Report screen for partition group 1.

2. 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.

3. Press **Cancel** to return to the command prompt.
4. Type **`change partition-route-table index 1`**. Press **Enter.**

   The system displays the Partition Routing Table screen. In our example, partition group 1 can make 1800 calls and these calls use route pattern 30.
5. In the **PGN2** column that corresponds to Route Index 1, type **30**. 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

To assign an extension to a partition group, first assign the partition group to a COR, and then assign that COR to the extension.

Instructions

To assign a Class of Restriction (COR) to partition group 2:

1. Type **`list cor`**. Press **Enter**.

   The system displays the Class of Restriction Information screen.

Figure 26: Class of Restriction Information screen

```
list cor                                                        page 1 of x
                    CLASS OF RESTRICTION INFORMATION

                   COR   COR Description
                    0
                    0    supervisor
                    2    telecommuting
                    3
```

2. Choose a COR that has not been used. Press **Cancel**.

   In our example, select **3**.
3. Type **`change cor 3`**. Press **Enter**.

   The system displays the **Class of Restriction** screen.

4. Type a name for this COR in the **COR Description** field.

   In our example, type **lobby**.
5. Enter **2** in the **Partitioned Group Number** field.
6. Press **Enter** to save your changes.

Now assign COR 3 to the lobby telephone at extension 1234:

1. Type **`change station 1234`**. Press **Enter**.

   The system displays the Station screen.
2. In the **COR** field, enter **3**.
3. Press **Enter** to save your changes.

Setting up Time of Day Routing

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.

Before you start

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.

Instructions

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:

1. Type **`display time-of-day 1`**. Press **Enter**.

   The system displays the Time of Day Routing Plan screen.

   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).

2. Press **Cancel** to clear the screen.

Now we will create a new time of day routing plan for long-distance calls for our executives.

1. Type **`change time-of-day 2`**. Press **Enter**.

   The system displays the Time of Day Routing Plan 2 screen.

2. 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.

3. 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.

4. Press **Enter** to save your changes.

Now assign your new Time of Day Routing Plan 2 to the COR assigned to your executives. See Class of Restriction in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, to see where to assign this field.

Example

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.

Related topics

See Route Pattern screens in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more information.

See Defining ARS Partitions on page 264 to see how to set up partition groups.

Location by Region

Location by Region provides a way to administer location by IP network region. This allows for the correct date and time information and trunk routing based on the IP network region.

Setting up a remote user by network region and time zone

Instructions

With your system located in New York and a remote user located in Germany, to create the correct time zone settings:

1. Type **`change locations`**. Press **Enter**.

   The system displays the **Locations** screen.
2. On line 11, in the **Name** field, enter the Communication Manager server associated with the location (for instance, **Germany**).
3. In the first **Timezone Offset** field, enter **+** to indicate the time is ahead of the system time.
4. In the second **Timezone Offset** field, enter **08** for the number of hours difference between this location and system time.
5. In the **Daylight Savings** field, enter **1** if this country has daylight savings.
6. Press **Enter** to save your changes.
7. Type **`change ip-network-map`**. Press **Enter**.

   The system displays the IP Address Mapping screen.

8. In the **From IP Address** field, enter the IP address for the remote station in Germany.
9. In the **To IP Address** field, enter the IP address of your system.
10. In the **Subnet or Mask** field, enter the subnet mask value of your network.
11. In the **Region** field, enter a number that is not being used. In this example, enter **3**.
12. Press **Enter** to save your changes.
13. Type **`change ip-network-region 3`**. Press **Enter.**

    The system displays the IP Network Region screen.
14. In the **Name** field, enter the location name for familiarity.
15. In the **Location** field, enter the number from the Locations screen. In this example, it was **11**.
16. Press **Next Page** until you get to the Inter Network Region Connection Management screen.
17. 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.
18. Press **Enter** to save your changes.

Related Topics

See *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205*,* for more information on the Multiple Locations feature.

Chapter 9: Managing 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 Communication Manager feature functionality to a Multimedia Communications Exchange (MMCX) system. MASI architecture fits the client/server model, where Communication Manager functions as a server for MMCX clients. Examples of features supported by MASI include call detail recording (CDR), CM Messaging voice mail integration, 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

Communication Manager/MASI features:

- Basic Call (Place/Drop) - Communication Manager tracks the status of all calls placed to or from a MASI terminal.
- Call Detail Recording - Communication Manager tracks calls to and from MASI terminals and can produce call records that indicate if a call uses MASI.
- Call Coverage - 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 - Communication Manager tracks conference calls that involve MASI terminals, if a Communication Manager station 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 Communication Manager World Class Routing capabilities.
- Voice messaging access to CM Messaging - MMCX users can take advantage of 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, Communication Manager can monitor traffic over those interfaces.

Before you start

CAUTION:
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.

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.

About this section

The following section describes the Multimedia Applications Server Interface (MASI), and provides instructions on how to set it up, including administration and monitoring. It also includes a section on troubleshooting.

You need to use both the DEFINITY Server system administration terminal (SAT) and the MMCX administration terminal to administer MASI. This document describes what you need to do at the DEFINITY Server SAT. It also occasionally mentions administration that you must do at the MMCX administration terminal. For more detailed MMCX information, see your MMCX documentation.

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."

Planning for MASI

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 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.

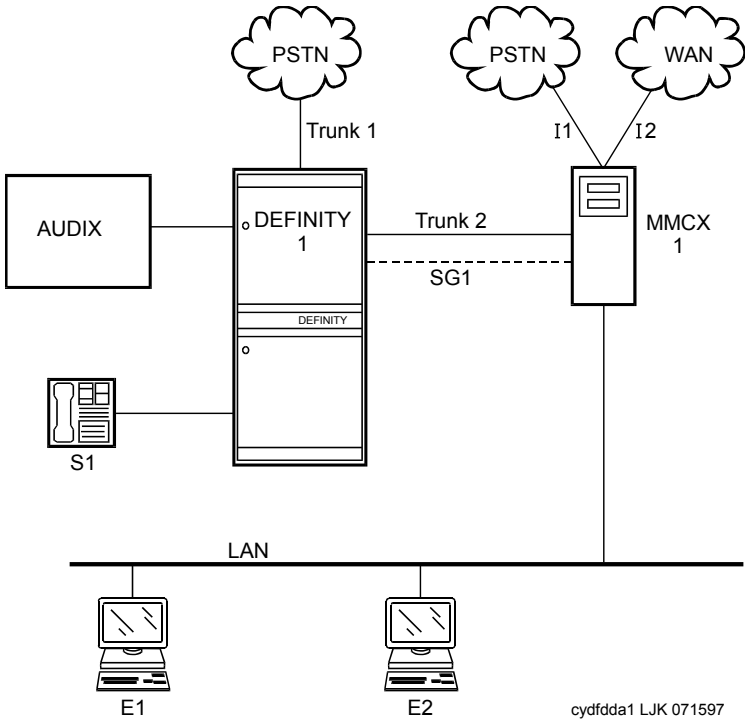
– one unused Communication Manager extension for the Near-End Path Termination number for all MASI Paths to this ECS. You can use the same number for all MASI nodes in the domain.

– 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.

MASI configurations

There are several ways to set up combinations of MASI nodes and DEFINITY servers.The following figures depict several possible configurations.

Figure 27: MASI domain of 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 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 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, Communication Manager informs the MMCX of its node number.
- S1 — Communication Manager station.

Figure 28: MASI domain of Communication Manager running on one DEFINITY Server and two (or more) MMCXs

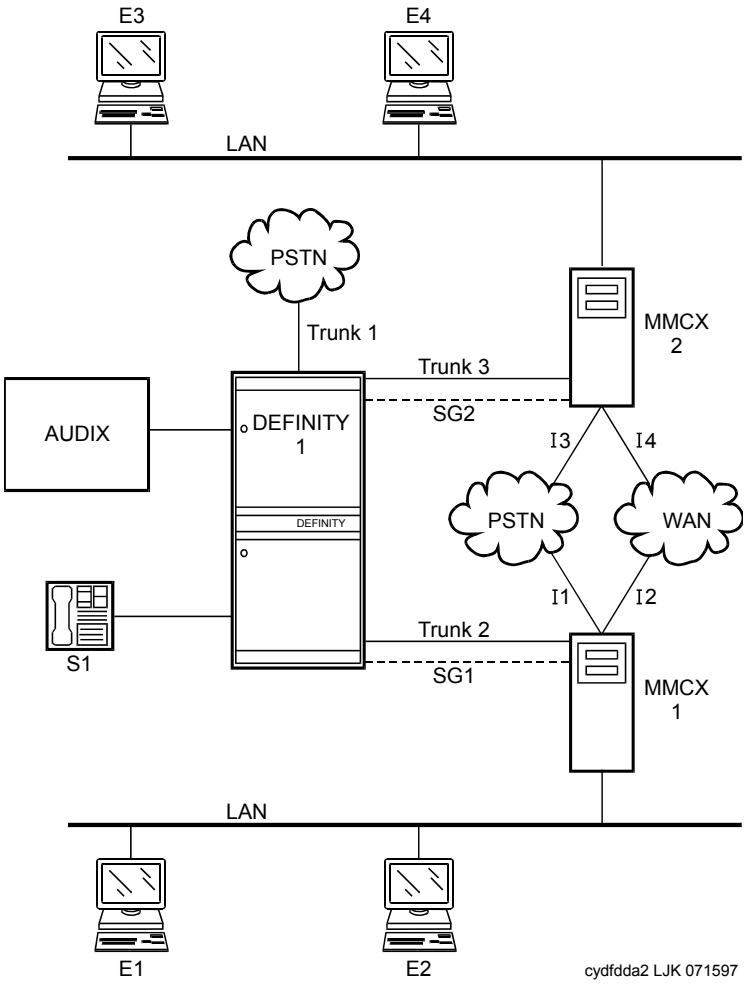


Figure 29: Two separate MASI domains

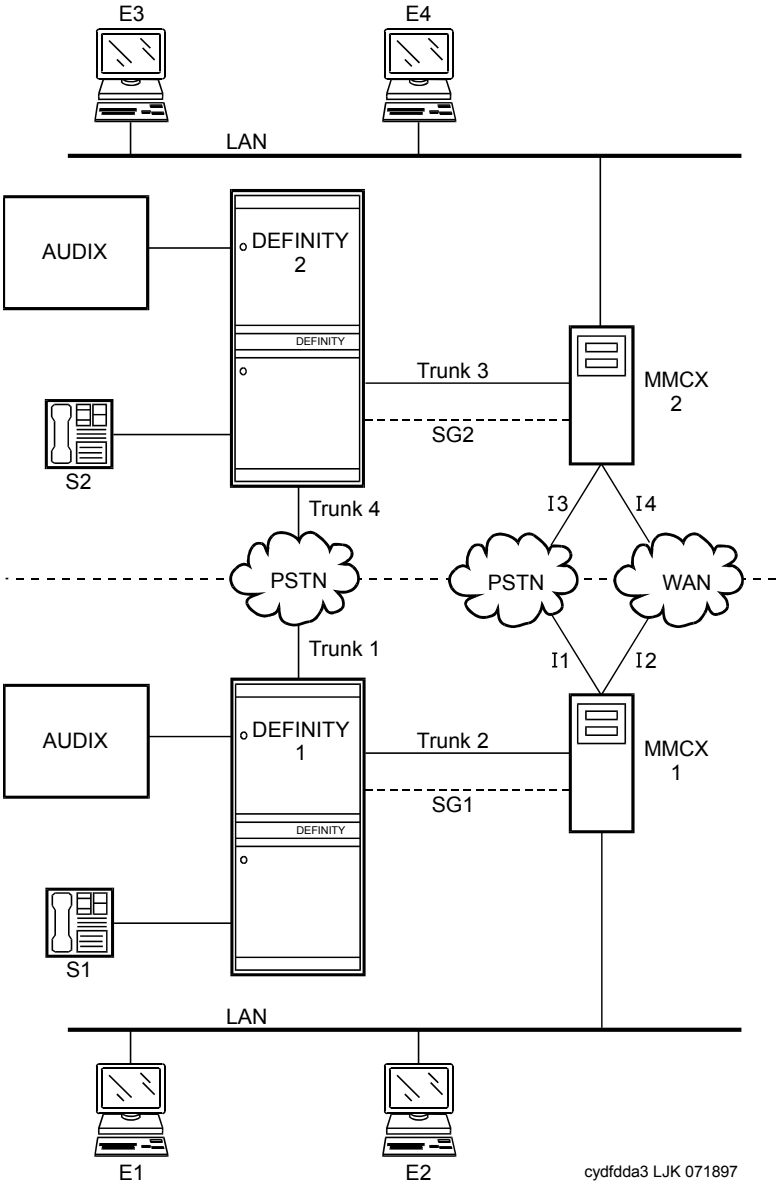
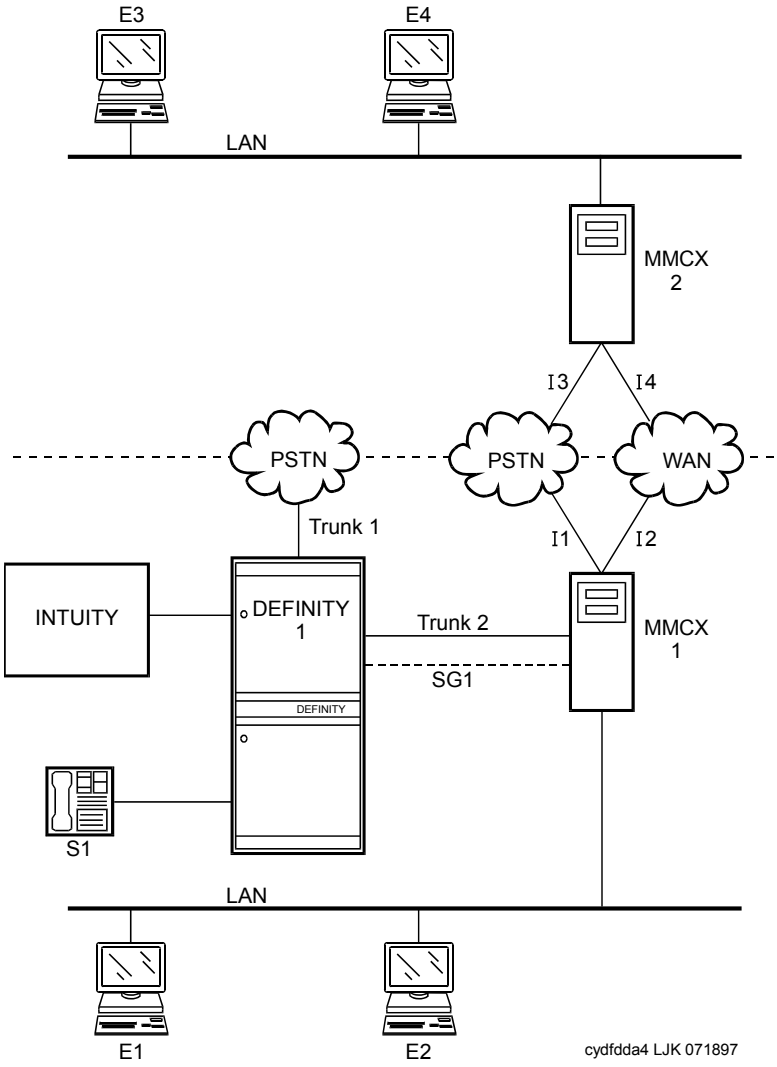


Figure 30: One MASI domain, and one non-MASI MMCX



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.

How to administer MASI

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.

Step 1 — Establishing customer options (Avaya)

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.

On the MMCX, MASI must be enabled using the **`chgmasi`** command.

Step 2 — Establishing maintenance parameters and alarming options (Avaya)

Ensure that on the Maintenance-Related System Parameters screen, the **Packet Bus Activated** field is **y**.

Using the **`set options`** command (Avaya *init* or *inads* logins only), set **MASI alarming options**. For more information, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300432.

Step 3 — Establishing the physical connection

Establish the physical connection between the Avaya DEFINITY Server and the MMCX.

Step 4 — Administering circuit pack

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

Step 5 — 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 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**, Communication Manager attempts to establish the connection as soon as you submit the screen. 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.

Figure 31: MASI Temporary Signaling Connections (TSC) Display

```
                    MASI TEMPORARY SIGNALING CONNECTIONS (TSC)

Sig.  Primary   TSC      Local                                          Mach.
Grp   D-Chan    Index    Ext.   Enabled  Established   Dest. Digits     ID

xxx   xxxxxxx   xxx      xxxxx     x     xxxxxxxx      xxxxxxxxxxxxxxx  xx
xxx   xxxxxxx   xxx      xxxxx     x     xxxxxxxx      xxxxxxxxxxxxxxx  xx
xxx   xxxxxxx   xxx      xxxxx     x     xxxxxxxx      xxxxxxxxxxxxxxx  xx
```

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

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.

Step 6 — Administer ISDN-PRI trunk group

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 Trunk Group in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Establish an ISDN-PRI trunk group with the following attributes:

Page 1

- 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.

Step 7 — Administer MASI Path Parameters

Use the **`change masi path-parameters`** command to access the MASI Path Parameters screen.

Figure 32: MASI Path Parameters screen

```
                         MASI PATH PARAMETERS

Near-End Path Extension: _____

    MASI Node      Trunk Group        Far-End Path Termination Number
        1              __                  __________________
        2              __                  __________________
        3              __                  __________________
        4              __                  __________________
        5              __                  __________________
        6              __                  __________________
        7              __                  __________________
        8              __                  __________________
        9              __                  __________________
       10              __                  __________________
       11              __                  __________________
       12              __                  __________________
       13              __                  __________________
       14              __                  __________________
       15              __                  __________________
```

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.

Step 8 — Administer MASI trunk groups

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 Communication Manager that are used for purposes other than MASI
- LAN interfaces linking MMCX servers

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 Communication Manager between 1 to 96 for DEFINITY Server CSI configurations.

Figure 33: MASI Trunk Group screen

```
                              MASI TRUNK GROUP

Group Number: 15                                          CDR Reports? y
  Group Name: INCOMING CALL_______________ COR: 1_     TN: 1        TAC: 915_

                               MASI Node Number: __  Remote Group Number: _
```

- **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`**.

Figure 34: List masi trunk-group output

```
                              MASI TRUNK GROUP

Group                                        Node    Remote
Number  TAC   Group Name                     Number  Grp No.  CDR  COR  TN

xxx     xxxx  xxxxxxxxxxxxxxxxxxxxxxxxxx     xx      x        x    xx   xxx
```

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.

Figure 35: Status masi trunk-group output

```
                             MASI TRUNK GROUP STATUS

        Group Number: xxx       Number of Active MMCX Trunk Calls: xxx
   MASI Node Number: xx
 Remote Group Number: xxx
```

Step 9 — Administer MASI terminals

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 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.

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 Communication Manager. If you do not, you will not be able to dial this extension from Communication Manager.

Figure 36: MASI Terminal screen — page 1

```
add masi terminal next

                           MASI TERMINAL

 Extension: 1000                                            BCC: 0
                                        MASI Node Number: __ TN: 1__
                                                            COR: 1_
      Name: ___________________________


 TERMINAL OPTIONS

        Send Display Info? y
```

- **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 Communication Manager should forward display information associated with a call. Set to **y**.

Figure 37: MASI Terminal screen — page 2

```
                              MASI TERMINAL

 FEATURE OPTIONS
            LWC Reception: none___

              CDR Privacy? n
```

- **LWC Reception** — This field indicates whether the terminal can receive Leave Word Calling (LWC) messages. Valid values are **none**, **audix**, **msa**, and **spe** (for DEFINITY Server CSI configurations). SPE-based LWC is not supported for MASI terminals. However, if CM Messaging 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 CM 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.

Figure 38: MASI Terminal screen — page 3

```
                              MASI TERMINAL
SITE DATA
       Room: _______
       Jack: _____
      Cable: _____
      Floor: _______
   Building: _______





BUTTON ASSIGNMENTS
 1: call-appr
```

- **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

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.

Figure 39: Duplicate MASI Terminal screen

```
                              MASI TERMINAL


Ext          Name                           Room      Jack  Cable
77777        ____________________________   _________ _____ _____
77778        ____________________________   _________ _____ _____
77779        ____________________________   _________ _____ _____
77781        ____________________________   _________ _____ _____
77782        ____________________________   _________ _____ _____
77783        ____________________________   _________ _____ _____
_____        ____________________________   _________ _____ _____
_____        ____________________________   _________ _____ _____
_____        ____________________________   _________ _____ _____
_____        ____________________________   _________ _____ _____
_____        ____________________________   _________ _____ _____
_____        ____________________________   _________ _____ _____
_____        ____________________________   _________ _____ _____
_____        ____________________________   _________ _____ _____
_____        ____________________________   _________ _____ _____
```

Listing MASI terminals

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.

Figure 40: List MASI Terminal output

```
                          MASI TERMINALS


                                      Node
       Ext   Name                     Number CDR COR TN

       xxxxx xxxxxxxxxxxxxxxxxxxxxxxx xx    x   xx  xxx
       xxxxx xxxxxxxxxxxxxxxxxxxxxxxx xx    x   xx  xxx
       xxxxx xxxxxxxxxxxxxxxxxxxxxxxx xx    x   xx  xxx
       xxxxx xxxxxxxxxxxxxxxxxxxxxxxx xx    x   xx  xxx
```

To view the active or idle status of a specific MASI terminal, use the command **`status masi terminal (extension)`**.

Figure 41: Status MASI terminal command

```
                            GENERAL STATUS

                 TYPE: MASI        Service State: active
            Extension: 54001
       MASI Node Number: 14
```

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, and so on), as well as other information about the extension.

Figure 42: List extension type

```
                             EXTENSION TYPE

                                                                Cv1/
 Ext   Type                 Name                    COR  TN  COS  Cv2
 ---   ----                 ----                    ---  --  ---  ----
 1234  masi-terminal                                1    1   1
 4077  term-masi-path-call
```

Step 10 — Administer features

AAR/ARS

1. AAR/ARS is an optional feature on Communication Manager, and you need to purchase this option to use it with MMCX. To verify that this feature is enabled, use the command **`display system-parameters customer-options`**. If it is not enabled, contact your Avaya representative.
2. The MMCX dial plan must use the same feature access codes as 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.
3. Include this feature access code in the **`chgmasi`** command.

CDR

1. To get call detail records for calls over MMCX interfaces, set **CDR Reports = y** on the MASI Trunk Group screen.
2. To get call records for calls over the ISDN-PRI trunk group, set **CDR Reports = y** on the ISDN-PRI Trunk Group screen.
3. 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.
4. 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**.

Coverage

To establish coverage from a MASI terminal to CM Messaging:

1. Use the MMCX user interface to enter the CM Messaging hunt group extension as the coverage point. You cannot use Communication Manager coverage administration for MASI terminals.
2. If CM Messaging ports are not administered in Communication Manager, you must administer them.
3. Set up the MASI terminal as a CM Messaging subscriber. Enter the MASI terminal extension in the **Extension** field on the Subscriber Administration screen.

To establish coverage from a MASI terminal to another MMCX terminal or Communication Manager station:

1. Use the MMCX user interface to enter the desired extension as the coverage point for the MASI terminal. You cannot use Communication Manager coverage administration for MASI terminals.

Step 11 — Verify administration

You should make test calls from Communication Manager to MMCX, to ensure that you can indeed place and receive calls.

Call an unattended MASI terminal. Verify that the call goes to CM Messaging. Retrieve the call from the MASI terminal. Verify that all works as expected.

Setting MASI command permissions

If you are the super-user for your system, you can restrict other administrative logins from changing MASI administration. To do this, use the **`change permissions (login-ID)`** command. 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

Using 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 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, 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 on page 278.

- 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. 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 a Communication Manager extension, including a CM Messaging hunt group, Callmaster agent, attendant console or telephone as their coverage point.

If CM Messaging is established as the MASI terminal's coverage point, the MASI terminal receives message waiting indication, and dials the CM Messaging hunt group extension to retrieve messages. Once connected to CM Messaging, 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.

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 CM Messaging directly, or that place calls to MASI terminals that cover to CM Messaging, do not receive ringback if all CM Messaging 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 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

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 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 Communication Manager for purposes of status and CDR records.

You cannot administer MASI trunks as part of Communication Manager route patterns.

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. Note the following CAUTION.

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 a 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.

Other interactions

The following section describes feature behaviors that might not be as expected, but that are not likely to be destructive.

Attendant features

- 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 Communication Manager trunks. However, you can administer these indicators for the trunk group administered for MASI paths.
- Attendant Trunk Identification — The attendant is not able to identify the trunk name via button pushes.

Basic features

- 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 — Communication 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 — 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 CM Messaging. You cannot administer SPE-based LWC. MASI terminals cannot send LWC messages to 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.
- Message Retrieval — MMCX users can only retrieve messages through CM messaging.

- Music on Hold — Music on hold will only be available if a 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 (CM Messaging) to another MASI terminal.

Hospitality features

- Do Not Disturb — MASI terminals cannot activate Do Not Disturb.

Multimedia features

- 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

Verify proper operation using the following commands and follow normal escalation procedures to resolve any failures detected by the demand test.

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. Also verify proper administration.
3. Verify the temporary signaling connection using the **`test tsc-administered <group number>`** command. Also verify proper administration.

Common error conditions

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.

You might want to use the **`busy port`** and **`release port`** commands to unlock things if features are not working.

Avaya 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 on page 309.

Detailed description of Avaya Video Telephony Solution

The Avaya Video Telephony Solution enables 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 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 S8300, S8500 and S8700-Series Server, see the procedures stated in the *Video Telephone Solution R3.0 Quick Set Up Guide*, 16-300310, Issue 3, February 2007.

Administering the Avaya Video Telephony Solution

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

This section describes:

- Any prerequisites for administering the Avaya Video Telephony Solution
- Complete administration procedures for the Avaya Video Telephony Solution

Prerequisites for administering Avaya Video Telephony Solution

You must complete the following actions before you can administer the Avaya Video Telephony Solution:

- 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.

- 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**

Configuring Video-Enabled Avaya IP Softphone Endpoints

To configure video-enabled Avaya IP Softphone endpoints:

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:
   - **Allow Direct-IP Multimedia** to **y**.
   - **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 to receive audio and video.
   - **Maximum Call Rate for Priority Direct-IP Multimedia** allows you to set the maximum call rate per call for priority users
   - Repeat this step for each IP codec set that will be used for video.
3. Type **`change cos`** and page 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:
   - **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.

5. Type **`add station`** command to add an Avaya IP Softphone station, and set the following parameters for that station:
   - **IP Softphone** to **y**.
   - **IP Video Softphone** to **y**.
   - **IP Audio Hairpinning** to **y**.
   - Repeat Step 5 for each video-enabled Avaya IP Softphone endpoint you want to configure.

Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems

To configure the Polycom VSX Video Conferencing systems and the V500 Video Calling Systems:

1. 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
2. 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.
3. 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

4. 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.
5. 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**.
6. 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.

7. Install the Polycom system and connect it to your network.
8. Upgrade the Polycom system software.
9. Using a web browser, access the Polycom home page for the unit, and select **Admin Settings**>**Network**>**IP Network**.
10. Select the **Enable IP H.323** check box.
11. Select the **Display H.323 Extension** check box.
12. In the H.323 Extension (E.164) box, enter the station number you specified for this system on the Communication Manager system.
13. From the Use Gatekeeper box, select **Specify with PIN**.
14. In the Gatekeeper IP Address box, enter the IP address of the C-LAN or PC LAN followed by***:1719*** to specify the correct port that must be used.
15. In the Authentication PIN box, enter the security code you entered in Step 4.
16. In the Number box in the Gateway area, enter the extension you specified in Step 10.
17. In the Type of Service box in the Quality of Section area, select IP Precedence.
18. 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.
19. Select the **Enabled PVEC** check box.
20. Select the **Enable RSVP** check box.
21. Select the **Dynamic Bandwidth** check box.
22. From the Maximum Transmit Bandwidth box, select the setting that matches the Maximum Call Rate for Direct-IP Multimedia setting you specified for the Communication Manager system.
23. From the Maximum Receive Bandwidth box, select the setting that matches the Maximum Call Rate for Direct-IP Multimedia setting you specified for the Communication Manager system.
24. Complete the Firewall and Streaming sections as necessary.
25. When finished, click the **Update** button.
26. Repeat the steps for each Polycom system.

Configuring Polycom PathNavigator Gatekeepers

To configure a Polycom PathNavigator gatekeeper:

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** command to put the gatekeeper in its own network region. 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 **IP**.
   - 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.

Configuring video trunks between two Communication Manager systems

To configure video trunks between two Communication Manager systems:

1. Use the **`change ip-codec-set 1`** command to set the following parameters:
   - Set **Allow Direct-IP Multimedia** to **y** (page 2 of screen).
   - 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.
   - **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 C-LAN or PC LAN 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 **n**.
- **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 **IP**.
   - 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.

Configuring the Maximum Bandwidth for Inter-Network Regions

To configure the maximum bandwidth for inter-network regions:

1. Type **`change ip-network region 1`**.
   The system displays the IP Network Region screen.
   Page down till you see the page titled Inter Network Region Connection Management.
2. 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:
   – To support audio only and no video, set the **Video** field to 0 and audio to a very high number.
   – To support audio and video with no bandwidth management, set both the **Total** and **Video** fields to No Limit.
   – To restrict audio bandwidth, and allow unlimited video bandwidth, set the **Total** field to the desired bandwidth. Set the **Video** field to No Limit.

- 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.
- Set priority video to the maximum bandwidth that can be used exclusively by priority video users

3. Figure 43 shows one possible usage scenario for Intervening-regions for network that are not directly connected by WAN. The values that you see are shown as an example.

Figure 43: Inter Network Region Connection Management screen

```
display ip-network-region 2                                    Page   3 of  19

                    Inter Network Region Connection Management

 src dst codec direct   Total           Video                            Dyn
 rgn rgn  set   WAN  WAN-BW-limits  Norm Prio  Shr Intervening-regions  CAC IGA
 2   1    2     y      10:Mbits        2     3  y                           n
 2   2    2
 2   3    2     n                                     4:  1:   :            n
 2   4    4     y      10:Mbits        2     2  y                           n
 2   5    5     y      10:Mbits        0     0  y                           n
 2   6    4     n                                     4:  1:  3:  7         n
 2   7
 2   8
 2   9
 2   10
```

Checking bandwidth usage

To check the status of bandwidth usage:

1. Type **`status ip-network-region`**.
   The system displays the Inter Network Region Bandwidth Status screen for a call that is up.

Figure 44: Inter Network Region Bandwidth Status screen

```
status ip-network-region 2/4

                     Inter Network Region Bandwidth Status
                                                   Number of   # Times
Src Dst  Conn    Conn  BW-limit   BW-Used(Kbits) Connections BW-Limit  IGAR
Rgn Rgn  Type    Stat                 Tx    Rx     Tx     Rx Hit Today Now/Today

  2   4 direct   pass   10 Mbits       0     0      0      0      0      0/  0
              Video:    2 Mbits       0     0      0      0      0
           Priority:    2 Mbits       0     0      0      0      0
```

2. 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.

Administering Ad-hoc Video Conferencing

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.

Administering ad-hoc video conferencing involves the following steps:

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.

Firmware video compatibility matrix

Vendor	Product	Version	Communication Manager version	
			4.0.3+	**5.0 SP3+**
Avaya	IP Video Softphone	R6 SP4+	Yes	Yes
	C-LAN	FW26+(2)	Yes	Yes
	Meeting Exchange	5.0.2.00 (4.13.0.2)	No	Yes
Vendor	**Product**	**Version**	**Communication Manager version**	
			4.0.3+	**5.0 SP3+**
Polycom	PathNavigator	7.00.08.0407+(6)	Yes	Yes
	SE200	3.00.02.ER019+(6)	Yes	Yes
	iPower	6.0.0.315+	Limited (3,4)	Limited (3,4)
	ViewStationFX	V6.0.5+	Limited (3)	Limited (3)
	ViewStation	V7.5.4+	Limited (3)	Limited (3)
	VSX/V500	8.7.1	Yes	Yes
		9.0+	Yes	Yes
	MGC	8.0.0.27	Yes	Yes
		9.0.1.8+	Yes	Yes
	RMX	2.0.2.25+		Yes
	HDX	2.0.2-2461+	Yes(5)	Yes
	RSS2000		No	No
Tandberg	T150	L5.0(7)	Yes	Yes

Key:

Blank=Unverified; Yes=Verified; No=Does not work; +=Later firmware

Notes:

(1) IPSP R6 video not backward compatible with CM3.1.2 and earlier.

(2) C-LAN FW11 has known issues with VSX registration.

(3) Telephony features and IPSP video mute are not supported.

(4) Internal MCU calls from an iPower to an IPSP, or Communication Manager connected VSX do not connect.

(5) CM4.0.1 SP1 required for HD video.

(6) Inter-gatekeeper call rate management requires CM4.0.4 or CM5.1.1 SP1 minimum.

(7) Until L5.2 is available, T150 requires dedicated ip-network-region with IP-IP Direct Audio set to no.

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 on page 297.

Operations in Basic or Enhanced modes

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.

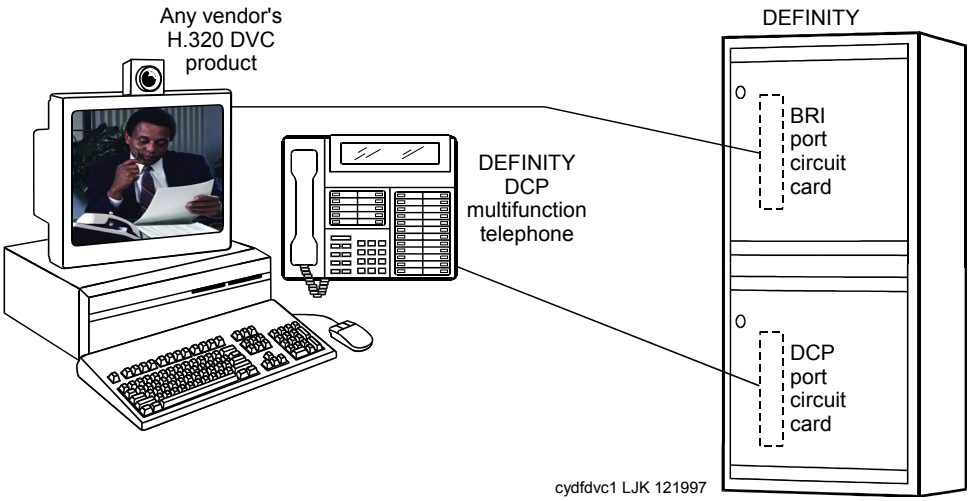
Definitions: MMCH features and components

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.

Figure 45: MMCH multimedia complex



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 complex provides a loose integration of the voice station and H.320 DVC system.

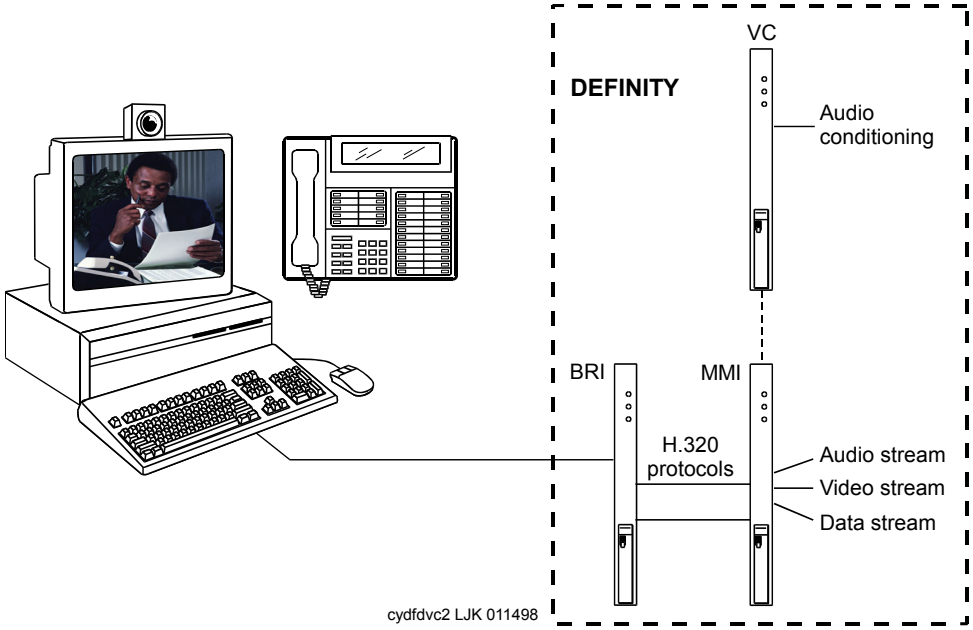
Enhanced multimedia complex

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 Communication Manager with a BRI line.

Figure 46: Enhanced MMCH service link



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."

Feature Description

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.

Basic Mode Operation

In Basic Mode:

- 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.

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."

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.

ESM Installation

Figure 47: Typical Multimedia Call handling ESM Connections

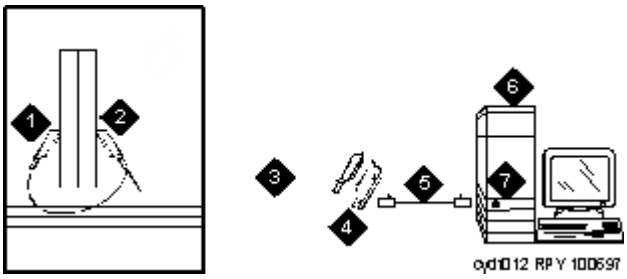


Figure notes:

1. Port B Y-cable connector to a TN787 multimedia interface (MMI) circuit pack
2. Port A Y-cable connector to a TN2207 PRI circuit pack
3. 25-pair Y-cable
4. 356A adapter
5. D8W cord connected to 356A adapter S/B port 8
6. Extended services module (ESM)
7. Port B on compatible primary rate interface (PRI) card

Use the following procedure and Typical Multimedia Call handling ESM Connections on page 314 to connect to the ESM equipment:

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 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.

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 on page 323). For information about these screens, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.
5. Configure the ESM adjunct.

Planning for MMCH

The following are some of the tasks you perform in planning and administering MMCH.

Planning the system

Questions to help you use Communication Manager for multimedia are:

- 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.

Installation checklist

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:
   - Install MMIs, VCs and the ESM.
   - Administer the ESM to ECS connection — DS1 Circuit Pack and Signaling Group screens.
   - Establish maintenance parameters — Maintenance-Related System Parameters screen.
6. Administer multimedia complexes:
   - Administer data modules — Data Module screen, or Data Module page of the Station screen.
   - 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

- 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)
  - 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.

Administering MMCH settings

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 on page 312).
  - 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 on page 312.

- **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 on page 330).

  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.

Assigning Multimedia Buttons

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.

- The mm-pcaudio feature can only be used via button.
- The **mm-cfwd** button can be replaced by the standard "*call forward*" FAC followed by the "*multimedia call*" FAC.
- **mm-call** -This 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. 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.

  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.
- **mm-basic** - This 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.

  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.

- **mm-pcaudio** - This 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). To switch the audio path to the PC while active on a call, the user presses the **mm-pcaudio** button (if off-hook you can now hang up the handset). 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.

  A user can simply go off-hook on their 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.

- **mm-datacnf** - Pressing the **mm-datacnf** button from any voice station that is participating in a multimedia call will light the status lamp 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.

- **mm-cfwd** - The **mm-cfwd** button allows 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.

- **mm-multinbr** - The **mm-multinbr** call button is similar to the **mm-call** button. It allows origination of a multimedia call from any 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 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.

ESM T.120 Server Administration

From the system administration terminal:

1. Type **`list configuration all`**, and 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), and the system displays the DS1 Circuit Pack screen.
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.
15. The **MMI Interface** field **ESM** appears.
16. Enter **`add signaling-group next`**. The system displays the Signaling Group screen.
17. Set the **Associated Signaling** field to **y**.

18. Set the **Primary D-Channel Port** field to ***xxxx*16** (where ***xxxx*** is the address of the TN2207 PRI circuit pack, for example: 1B0516).
19. The **Max Number of NCA TSC** default is **0**.
20. The **Max Number of CA TSC** default is **0**.
21. **Trunk Group for NCA TSC ____** (leave blank).
22. **Trunk Group for Channel Selection____** (leave blank).
23. Logoff the terminal and then log back on the terminal to view your changes.

Troubleshooting

To determine ESM link status, enter the following commands from the system administration terminal:

1. **`Status esm`**
2. **`Status signaling-group`**
3. **`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, Communication Manager directs it to the telephone. If the incoming call is 56K or 64K data call, 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.

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, and so on. 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, and so on.

   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, and so on. 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, and so on. 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, and so on. 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, and so on.

   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, and so on.

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
   1. Single address with TAC
      - ***Dial*** **mm-call** button or FAC, ***Hear*** dialtone
      - ***Dial*** TAC, **Dial** destination digits
   2. 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
   3. Single address with AAR/ARS
      - ***Dial*** **mm-call** button or FAC, ***Hear*** dialtone
      - ***Dial*** AAR/ARS, ***Dial*** destination digits
   4. 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
   5. 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
   6. Dual address with AAR/ARS and authorization code
      - ***Dial*** **mm-multinbr** button or FAC, ***Hear*** dialtone
      - ***Dial*** AAR/ARS FAC, **Dial** 1st dest. digits, ***Hear*** dialtone
      - ***Dial*** AAR/ARS FAC, **Dial** 2nd dest. digits, ***Hear*** stutter dialtone
      - ***Dial*** authorization code
   7. 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, ***Hear*** destination digits

8. 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

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.

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 Connections

Basic Multimedia endpoints can serve as the origination point or destination of an administered connection.

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). 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

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.

To set up a multimedia conference:

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 CM Messaging 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 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

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 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. 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.
3. 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. 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, and so on. 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 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 DEFINITY Server or 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 (that is the server which activated **mm-datacnf**) can be any combination of Enhanced multimedia complexes, Basic multimedia complexes or stand-alone H.320 DVC systems. *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

In Basic mode you can forward calls from either the telephone or the multimedia endpoint. To forward a call from the multimedia endpoint:

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, 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

Members of a pickup group can answer an H.320 call using a telephone after the call has been converted to voice. This is true for standard or 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

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 (that is 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. 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 (that is 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

Incoming Basic mode data calls follow established night-service processing for data calls.

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 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.

1-number access

1-number access permits originating users to make voice or multimedia calls to an Enhanced multimedia complex by dialing the same number for either type of call. The number can be the voice station extension or the data module extension. If the incoming call is a voice call, Communication Manager alerts the station of an incoming voice call. If the incoming call is 56K or 64K data call, Communication Manager recognizes it as a multimedia call, inserts resources to terminate the H.320 protocol, and alerts the voice station with a multimedia call.

Calls originating on the same Avaya S8XXX Server as the Enhanced 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 non-PRI digital facilities for data, multimedia calls must be made to the data extension of the Enhanced mode complex.

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.

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

Multimedia calls from an Enhanced multimedia complex are originated from the VOICE 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, and so on. 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, and so on.

   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, and so on. 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, and so on. 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, and so on. 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, and so on.

   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, and so on.

   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

   1. Single address with TAC
      - ***Dial*** **mm-call** button or FAC, ***Hear*** dialtone
      - ***Dial*** TAC, ***Dial*** destination digits
   2. 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
   3. Single address with AAR/ARS
      - ***Dial*** **mm-call** button or FAC, ***Hear*** dialtone
      - ***Dial*** AAR/ARS, ***Dial*** destination digits
   4. 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
   5. 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

6. 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
7. 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
8. 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.

Creating 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.

The following steps create a multi-party voice/video conference:

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 (that is uses the mm-call button/FAC/and so on.) 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 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.

The following steps add data sharing to a video conference:

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. 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, and so on. 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.

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.

Single server or switch data collaboration.

When all parties involved in data collaboration conference are located on the same physical Avaya DEFINITY Server or 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 (that is the server that 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 (that is 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.

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 CM Messaging 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 (that is 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.

Figure 48: General Status screen

```
status station nnnn                                          page 1 of x

                           GENERAL STATUS

              Type: 7405D              Service State: in-service/on-hook
         Extension: 1002            Maintenance Busy? no
              Port: 01C0702            SAC Activated? no
       Call Parked? no              User Cntrl Restr: none
  Ring Cut Off Act? no             Group Cntrl Restr: none
Active Coverage Option: 1         CF Destination Ext:
                                     MM Conference ID:
                                       MM Endpoint ID:
   Message Waiting:
   Connected Ports:

             ACD STATUS                       HOSPITALITY STATUS
    Agent Logged In   Work Mode           AWU Call At:
                                             User DND: not activated
                                            Group DND: not activated
                                          Room Status: non-guest room
       On ACD Call? no
```

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.

Figure 49: List Multimedia Endpoints screen

```
            MULTIMEDIA ENDPOINTS

Data Ext     MM Complex Voice Ext     H.320 Conversion?

100                  87654                    y
1321
15683                738                      n
```

Figure 50: List Multimedia H.320-Stations screen

```
                  MULTIMEDIA H.320-STATIONS

       Station Ext             MM Data Ext

          100                     87654
        1321
          15683                   738
```

Figure 51: List Multimedia IP-Stations screen

```
                  MULTIMEDIA IP STATIONS

           IP STATION             MEDIA COMPLEX
   Ext   Port   Registered?    Ext    Port    Registered?
    100              y       87654                  y
    1321
    15683            n       738                    n
```

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 10: Setting Up Telecommuting

Configuring Communication Manager for Telecommuting

Telecommuting emphasizes the ability to perform telephony activities while remote from Communication Manager. It is a combination of four features which 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 on page 88 for more information.

- Coverage of Calls Redirected Off Net (CCRON) 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.

Before you start

You can also set up telecommuting with an IP (internet protocol) telephone or IP Softphone. For example, see Adding an H.323 Softphone on page 88 for more information.

For DCP/ISDN telecommuting, ensure 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.

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 **Avaya Communication Manager extender** nor the System Parameters Customer-Options **(Optional Features)** fields are configured, contact your Avaya technical support representative.

Verify the telecommuting access extension is a direct inward dialing (DID) or a central office (CO) trunk destination for off-premises features to work.

Configure **TTI** for personal station access (PSA). For information about configuring TTI, see Setting up Personal Station Access on page 365.

Configure Security Violation Notification for Station Security Codes. For information about Security Violation Notification, see Setting up Security Violations Notification on page 395.

Instructions

In our example, we set up the telecommuting extension and enable coverage of calls redirected off-net.

To configure Communication Manager for telecommuting:

1. Type **`change telecommuting-access`**. Press **Enter**.

   The system displays the Telecommuting Access screen.

2. In the **Telecommuting Access Extension** field, type **1234**. Press **Enter**.

   This is the extension you are configuring for telecommuting.

3. Type **`change system-parameters coverage`**. Press **Enter**.

   The system displays the System Parameters Call Coverage/Call Forwarding screen.

4. In the **Coverage Of Calls Redirected Off-Net Enabled** field, type **y**. Press **Enter**.

Related topics

See Telecommuting Access in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for information about and field descriptions on the Telecommuting Access.

Setting up Personal Station Access

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.

Before you start

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.

Verify that the extension has a COS that allows PSA.

Instructions

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.

To set up Personal Station Access:

1. Type **`change system-parameters features`**. Press **Enter**.

   The Feature-Related System Parameters screen appears.
2. Complete the following fields. Press **Enter**.
   a. Type **voice** in the **TTI State** field.
   b. (Optional) Type **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. Type **`change cos`**. Press **Enter**.

   The Class of Service screen appears.
4. Type **y** in the **Personal Station Access (PSA) 1** field. Press **Enter**.
5. Type **`change feature-access-codes`**. Press **Enter**.

   The Feature Access Code (FAC) screen appears.
6. Complete the following fields. Press **Enter**.
   a. Type **#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. Type **#3** in the **Dissociate Code** field.

This is the feature access code you will use to deactivate Personal Station Access at a telephone.

More information

You can allow users to place emergency and other calls from telephones that have been dissociated. To enable this, you must first assign a class of restriction (COR) for PSA-dissociated telephones. You do this on the Feature-Related System Parameters screen. In addition, you must 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.

Related topics

See Changing Telecommuting Settings on page 378 for information on how to associate or disassociate PSA.

See Setting Up Enterprise Mobility User on page 143 for information on how to set up the Enterprise Mobility User feature.

Creating a Station Security Code

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.

Instructions

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.

To create a station security code:

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

   The system displays the Feature Access Code (FAC) screen.

2. Type **#5** in the **Station Security Code Change Access Code** field. Press **Enter**.

   This sets the access codes for this features. The Command prompt appears.

3. Type **`change system-parameters security`**. Press **Enter**.

   The system displays the Security-Related System Parameters screen.

4. Type **4** in the **Minimum Station Security Code Length** field. Press **Enter**.

   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. Type **`change station 1234`**. Press **Enter**.

   This is the station extension you configured for telecommuting. The system displays the Station screen.

6. Type **4321** in the **Security Code** field. Press **Enter**.

Related topics

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

Communication Manager allows you assign an extender password to a user. You can assign one password for each Communication Manager port.

Before you start

Use the Remote Extender PC in the server room to perform this procedure.

Instructions

In this example, we will set a system-generated random password for a user named John Doe.

To assign an extender password:

1. Double-click the **Security** icon.

   The system displays the Password Manager screen.
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. Type **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**.

   The system returns you to the Password Manager screen.
8. Select **CommLink:Upload Password**.

   The error message screen appears with the message **Administrator password not loaded"**.
9. Click **OK**.

   The system displays the Administrator screen.
10. Type **123456** and click **OK**.

    This is the administrator's password.
11. Select **CommLink:Upload Password**.

    The password is uploaded.
12. When upload is complete, click **OK**.

    The system returns you to the Password Manager screen.
13. Select **File:Save As**.

    The Save As screen appears.

14. Type **doe.fil** in the **File** field and click **OK**.

    The system saves the User01 information.

Setting up Call Forwarding

Communication Manager allows you to change your call forwarding from any on-site or off-site location.

Instructions

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.

To set up call forwarding:

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

   The system displays the Feature Access Code (FAC) screen.
2. Set a 2-digit access code for the following fields. Press **Enter**.
   a. Type ***8** in the **Extended Call Fwd Activate Busy D/A** field.
   b. Type ***7** in the **Extended Call Fwd Activate All** field.
   c. Type ***6** in the **Extended Call Fwd Activate Deactivation** field.

      This sets the access codes for these features. The Command prompt appears.
3. Type `change cos`. Press **Enter**.

   The system displays the Class of Service screen.
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**. Press **Enter**.

   This allows your users to forward calls off-site.

Interactions

- 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.

Related topics

See Changing Telecommuting Settings on page 378 for information on how to change call forwarding.

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.

Assigning Coverage Options

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 on page 184. For information about creating a time of day coverage table, see Assigning a coverage path to users on page 185.

Instructions

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.

To assign 2 coverage options:

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

   The system displays the Feature Access Code (FAC) screen.
2. Type **#9** in the **Change Coverage Access Code** field. Press **Enter**.
3. Type **`change cor 1`**. Press **Enter**.

   The system displays the Class of Restriction screen.
4. In the **Can Change Coverage** field, type **y**. Press **Enter** to save your work.

   The Command prompt appears.
5. Type **`change station 1234`**. Press **Enter**.

   This is the station extension you configured for telecommuting. The Station screen appears.
6. Complete the following fields:
   a. Type **2** in the **Coverage Path 1** field.
   b. Type **8** in the **Coverage Path 2** field.

Related topics

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 Changing Telecommuting Settings on page 378 for information on how to alternate your coverage path option.

See *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205, for information about the Extended User Administration of Redirected Calls feature.

Installing Home Equipment

Communication Manager allows you to install equipment in your home so that you can utilize system facilities from off-site.

Before you start

You can also set up telecommuting with an IP (internet protocol) telephone or IP Softphone. For example, see Adding an H.323 Softphone on page 88 for more information.

For DCP telecommuting, you need the following equipment:

- Communication Manager extender remote module
- DCP sets (office and home must match)

Configure a feature access code for associating your home number to your office number. For information about configuring an associate feature access code, see Setting up Personal Station Access on page 365.

Instructions

Installing home equipment

To install your home equipment:

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. Type **5551234**. 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 display **Enter Password** appears.

9. Type **0123456789**. Press **Drop**.

Associating your office telephone number to the home station

To associate your telephone number:

1. On your home station, type **#4**.

   This is the associate feature access code.

2. Type **4321**. Press **#**.

   This is your extension number.

3. Type **1996**. Press **#**.

   This is your password.

Disassociating your home station

To disassociate your home station:

1. Press **Hold** four times.

Related topics

See Configuring Communication Manager for Telecommuting on page 363 for step-by-step instructions on how to configure your office equipment.

See Changing Telecommuting Settings on page 378 for step-by-step instructions on how to use your home station.

Setting up Remote Access

Remote Access permits a caller located outside the system to access the server running Communication Manager through the public or private network and then use the features and services of the system.

Remote Access users can dial into the system using central office (CO), Foreign Exchange (FX), Wide Area Telecommunications trunks (WATS), and Integrated Services Digital Network Primary Rate Interface (ISDN-PRI) trunks. In addition, a dedicated Remote Access Direct Inward Dialing number can be provided.

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.

Before you start

Configure the **Incoming Destination** and **Night Service** fields on the CO Trunk screen. For information about configuring a CO trunk, see Adding a CO, FX, or WATS trunk group on page 407.

Verify that the **Authorization Codes** field on the System Parameters Customer-Options **(Optional Features)** screen is set to **y**.

Verify that the **SVN Authorization Code Violation Notification Enabled** field on the Security-Related System Parameters screen is set to **y**.

Instructions

Setting up remote access

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.

To set up remote access:

1. Type **`change remote-access`**. Press **Enter**.

   The system displays the Remote Access screen.

2. Type **1234** in the **Remote Access Extension** field.

   This is the extension specified in the **Incoming Destination** field on the CO Trunk screen.

3. Type **7** in the **Barrier Code Length** field.

   This is the number of digits your barrier code must be when entered.

4. Type **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 Setting up Authorization Codes on page 392.

5. Type **y** in the **Remote Access Dial Tone** field.

   This means you hear dial tone as a prompt to enter your authorization code.

6. Type **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. Type **1** in the **TN** field.

   This is the Tenant Partition (TN) number.

9. Type **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 **01/01/04** 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. Type **y** in the **Disable Following A Security Violation** field.

    This disables the remote access feature following detection of a remote access security violation.

12. Press **Enter** to save your work.

Disabling remote access permanently

To disable remote access permanently:

1. Type **`change remote-access`**. Press **Enter**.

   The system displays the Remote Access screen.

2. Type **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. Press **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.

Using Secure Shell for remote login

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

- G350 Media Gateway
- S8300, S8400, S8500, or S8700-Series Server 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. For details on disabling Telnet, see Turning off Telnet for increased security.

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.

More information

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 Setting up Authorization Codes on page 392.

Related topics

See *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205, for a description of the Remote Access feature.

Changing Telecommuting Settings

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.

Before you start

Configure PSA. For information about configuring PSA, see Setting up Personal Station Access on page 365.

Assign two coverage options for your system. For information on how to assign coverage options, see Assigning Coverage Options on page 372.

Configure call forwarding for your system. For information about configuring call forwarding, see Setting up Call Forwarding on page 370.

Configure security codes for a station. For information about configuring personal station security codes, see Assigning an Extender Password on page 368.

Instructions

Associating PSA

In this example, we associate PSA (preferences and permissions) assigned to your station with another compatible terminal.

To associate PSA:

1. Dial **#4**.

   This is the associate PSA feature access code. You hear dial tone.

2. Type **1234**. Press **#**.

   This is your extension.

3. Type **4321**. Press **#**.

   This is your Station Security Code. You hear a confirmation tone.

Disassociating PSA

In our example, we disassociate PSA from the station you are using.

To disassociate PSA:

1. Dial **#3**.

   This is the disassociate PSA feature access code. You are no longer PSA associated to this station.

Changing a coverage option

In this example, we change the coverage option from path 1 to path 2 from a remote location.

To change a coverage option:

1. Dial **1234**.

   This is the extension you configured for telecommuting. You hear dial tone.

2. Dial **#9**. Press **#**.

   This is the feature access code you set for changing a coverage path. You hear dial tone.
3. Dial **4321**. 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

In this example, we change call forwarding to extension 1235.

To change call forwarding:

1. Dial **1234**.

   This is the extension you configured for telecommuting.
2. Dial **#8. Press #**.

   This is the feature access code you set for activating extended call forward. You hear dial tone.
3. Dial **4321**. Press **#**.

   This is the extension from which you want to forward calls.
4. Dial **87654321**. 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

In this example, we change the security code for extension 1235 from 98765432 to 12345678.

To change your security code:

1. Dial **#5**.

   This is the feature access code you set for changing your security code. You hear dial tone.
2. Dial **1235**. Press **#**.

   This is the extension for which you want to change the security code.

3. Dial **98765432**. Press **#**.

   This is the current security code for the extension. You hear dial tone.

4. Dial **12345678**. 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

To interrupt the command sequence for personal station security codes:

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 step1.
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.

Related topics

See *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205, for a description of the Security Violations Notification (SVN) feature.

Chapter 11: Enhancing System Security

Basic Security

Keeping 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.

- 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.
- 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.
- 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).
- 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.

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.

Preventing Toll Fraud

Top 15 tips to help prevent toll fraud

Toll Fraud Tips:

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 payphones located in subways, shopping malls, or airport locations. See Setting up Security Violations Notification on page 395 to prevent this happening to your company.

Physical Security

Physical security is your responsibility. Implement the following safeguards as an added layer of security:

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.

System Security Checklist

Here's some of the steps required for indemnification. Use these to analyze your system security.

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, type **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**, 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 Collecting Information About Calls on page 579 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 CM 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.

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*, 03-300431.

Using 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.

Using Busy Verify

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.

Before you start

On the Trunk Group screen - page 1, verify the **Dial Access** field is **y**. If it is not, contact your Avaya technical support representative.

Instructions

To use busy verify:

1. Type **`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, type **verify**.
3. Press **Enter** to save your changes.
4. To activate the feature, press the **Verify** button on the telephone and then enter the Trunk Access Code and member number to be monitored.

Setting up Authorization Codes

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.

Before you start

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.

Instructions

To set up authorization codes:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
2. Click **Next** until you find the **Authorization Code Enabled** field.
3. In the **Authorization Code Enabled** field, type **y**.

   This enables the Authorization Codes feature on a system-wide basis.
4. In the **Authorization Code Length** field, type **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, type **n**.

   This prevents the authorization code from displaying on telephone sets thus maximizing your security.
8. Press **Enter** to save your changes.
9. Type **`change authorization-code`** ***`nnnn`***, where ***`nnnn`*** is the authorization code. Press **Enter**.

   The system displays the Authorization Code - COR Mapping screen.
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. Type **`change trunk-group n`**, where ***n*** is the assigned trunk group number. Press **Enter**.

    The system displays the Trunk Group screen.

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. Press **Enter** to save your changes.

Related topics

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.

Setting up Security Violations Notification

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.

Instructions

To set up Security Violations Notification:

1. Type **`change system-parameters security`**. Press **Enter**.

   The system displays the **Security-Related System Parameters screen**.

2. In the **SVN Login Violation Notification Enabled** field, type **y**.

   This sets Security Violations Notification login violation notification.

   Note:
   If you are not using Security Violation Notification for logins, type **n** in the **SVN Login Violation Notification Enabled** field and go to Step 6.

3. In the **Originating Extension** field, type **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, type **attd** to send all calls to the attendant.

   This is the telephone extension that receives the referral call when a security violation occurs.

5. Press **Enter** to save your changes.

   Note:
   If you are not using Remote Access, go to Step 9.

6. (Optional) Type **`change remote-access`**. Press **Enter**.

   The system displays the **Remote Access** screen.

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. Press **Enter**.

   The system displays the Station screen.

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.

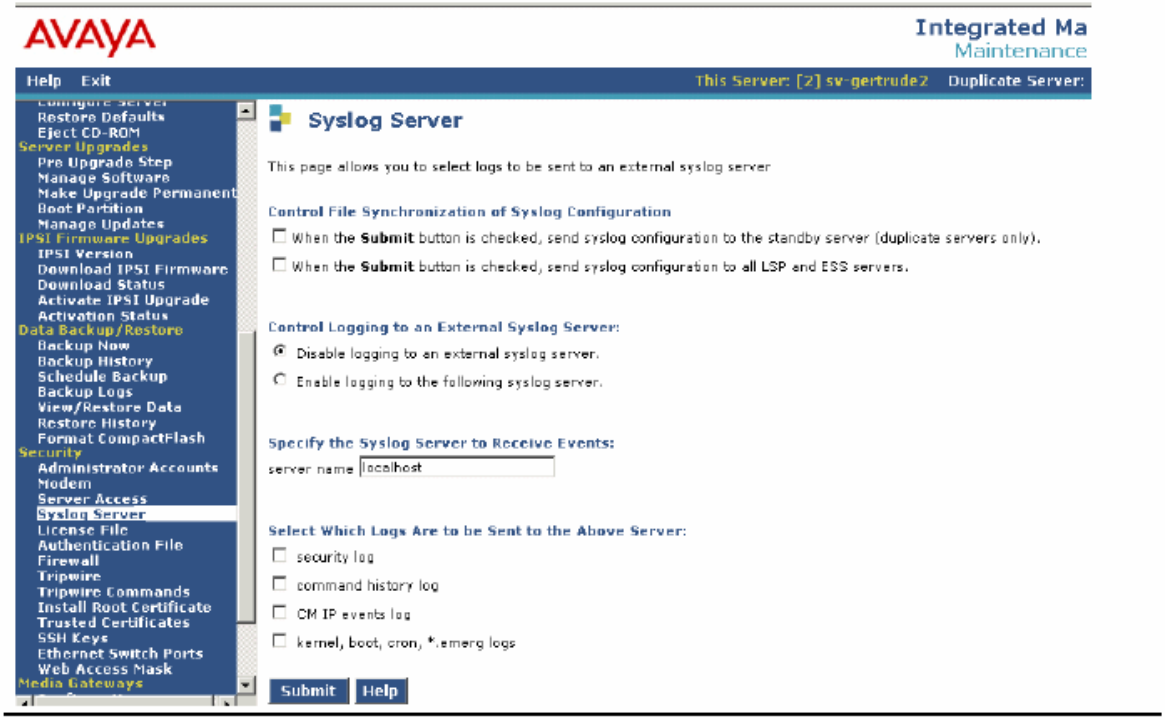
Enhanced security logging

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. Figure 52 shows the Syslog Server screen with the options that you can administer for this feature.

Figure 52: Syslog Server web page



Using 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 feature access code (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.

If a digital telephone has a feature button for Station Lock, but uses a FAC to activate the feature, the LED lights. The system does not generate the special tone.

If a digital telephone does not have a feature button for Station Lock, and uses a FAC to activate the feature, the system generates the special tone.

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.

Note:
Avaya recommends digital telephones use a Station Lock button rather than a feature access code.

Setting Station Lock

We will set Station Lock to allow authorized users to access the system through a particular station.

Before you start

- Be sure the **Station Lock COR** field on the Class of Restriction screen has the COR the user is using to define the calling restrictions.

Instructions

We will set Station Lock on a digital telephone (extension 7262):

1. Type `change station 7262`. Press **Enter**.
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. Press **Enter** to save your changes.
5. Type `change cor 1`. 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. Press **Enter** to save your changes.

9. Type **`change cor 2`**. Press **Enter**.
10. In the **Calling Party Restriction** field, verify it is **outward**.
11. Press **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.

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):

1. Type **`change station 7262`**. Press **Enter**.
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. Press **Enter** to save your changes.
4. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System-Parameters screen.
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`**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen.
8. Move the cursor to the **Station Lock Activation** field.
9. In the **Activation** field, type ***08**.
10. In the **Deactivation** field, type **#08**.
11. Press **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 T**ime 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 Service (COR) that allows the user to activate Station Lock with a feature access code (FAC).	**Station Lock COR**
Feature Access Code (FAC)	Assign a FAC for Station Lock.	**Station Lock Activation**

Screen name	Purpose	Fields
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
	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**

Dealing with Security Violations

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

You might have to enable Remote Access that has been disabled following a security violation, or disabled manually.

1. Log in to Communication Manager using a login ID with the correct permissions.
2. Type **`enable remote-access`**. Press **Enter**.

Disabling remote access

There might be occasions when you have to disable remote access for one of your users because of a security violation.

1. Log in to Communication Manager using a login ID with the correct permissions.
2. Type **`disable remote-access`**. Press **Enter**.

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.

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

Personal Station Access

The Hot Desking Enhancement (HDE) feature displays PSA Login information. You can invoke Personal Station Access (PSA) using H.323 IP telephones. If the HDE feature 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 H.323 telephones, if the **Hot Desking Enhancement Station Lock** field on the Feature-Related System Parameters screen is set to **y**.

The message used for displaying the PSA Login information is a non-call associated message, which appears at the top of an H.323 telephone.

The **Hot Desking Enhancement Station Lock** field on the Feature-Related System Parameters screen controls the feature.

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

Station Lock

Communication Manager Release 5.2 makes more restrictions available on the Station Lock feature. When the HDE feature is activated, the following are restricted:

- Access to telephone capabilities (applies to 96xx H.323 IP telephones with firmware changes)

- Call log
- Avaya menu
- Contact list
- USB access
- Redial button
- Bridging on Extension to Cellular calls
- Access to bridged appearances

Additionally, enabling the HDE feature by using the **Hot Desking Enhancement Station Lock** field in the Feature-Related System Parameters screen locks further capabilities. The capabilities are distributed among the telephone and Communication Manager.

Telephones

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 12: 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

Trunking technology is complex. Following a process can prevent mistakes and save you time. To set up new trunks and trunk groups, Avaya recommends following the process below (some steps might not apply to your situation):

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. Using the trunk access code, place a variety of calls.

This chapter provides instructions for steps 3 and 4 in this process.

Working with your network service provider

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.

Keeping records

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 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.

Related topics

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.

See Modifying Call Routing on page 260 for detailed information on Automatic Route Selection.

Adding a CO, FX, or WATS trunk group

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.

Before you start

Before you can administer any trunk group, you must 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.

Instructions

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

To add the new CO trunk-group:

1. Type **`add trunk-group next`**. Press **Enter**.

   The system displays the Trunk Group screen. 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, type **co**.

   This field specifies the kind of trunk group you're creating.

3. In the **Group Name** field, type **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, type **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, type **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, type **two-way**.

   This field defines the direction of traffic flow on this trunk group.

7. In the **Night Service** field, type **1234**.

   This field assigns an extension to which calls are routed outside of business hours.

8. In the **Incoming Destination** field, type **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, type **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, type **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, type **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, type **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. Press **Enter** to save your changes.

Now you are ready to add trunks to this trunk group. See Adding trunks to a trunk group on page 420.

Adding a DID trunk group

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.

Before you start

Before you can administer any trunk group, you must 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.

Instructions

To add the new Direct Inward Dialing (DID) trunk-group:

1. Type **`add trunk-group next`**. Press **Enter**.

   The system displays the Trunk Group screen. 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, type **did**.

   This field specifies the kind of trunk group you're creating.

3. In the **Group Name** field, type **Incoming calls**.

   You can type any name up to 27 characters long in this field.

4. In the **COR** field, type **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, type **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, type **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, type **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. Press **Enter** to save your changes.

Now you're ready to add trunks to this trunk group. See Adding trunks to a trunk group on page 420.

Related topics

See Inserting and absorbing digits on page 423 for instructions on matching modifying incoming digit strings to match your dial plan.

Adding a PCOL trunk group

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.

Before you start

Before you can administer any trunk group, you must 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.

Instructions

As an example, we will set up a new PCOL group and administer the group as a CO trunk for two-way voice traffic.

To add the new PCOL group:

1. Type **`add personal-co-line next`**. Press **Enter**.

   The system displays the Personal CO Line Group screen.

2. In the **Group Type** field, type **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, type **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, type **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, type **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, type **01D1901**.

   This is the port to which the trunk is connected.

7. In the **Trunk Termination** field, type **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, type **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. Press **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:

More information

Call Detail Recording

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.

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.
- CM 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.

Adding a Tie or Access trunk group

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.

Before you start

Before you can administer any trunk group, you must 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.

Instructions

As an example, we will add a two-way tie trunk group that supports voice and voice-grade data.

To add the new tie trunk-group:

1. Type **`add trunk-group next`**. Press **Enter**.

   The system displays the Trunk Group screen. 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, type **tie**.

   This field specifies the kind of trunk group you're creating.

3. In the **Group Name** field, type **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, type **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, type **105**.

   This field defines a unique code users can dial to access this trunk group.

6. In the **Direction** field, type **two-way**.

   This field defines the direction of traffic flow on this trunk group.

7. In the **Night Service** field, type **1234**.

   This field assigns an extension to which calls are routed outside of business hours.

8. In the **Comm Type** field, type **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, type **rbavd** in this field.

9. In the **Trunk Type** field, type **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. Type **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. Press **Enter** to save your changes.

Now you're ready to add trunks to this trunk group. See Adding trunks to a trunk group on page 420.

Adding a DIOD trunk group

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.

Setting up digital trunks

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.

Before you start

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 on page 419.

Before you can administer a digital trunk group, you must 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.

Instructions

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:

1. Type **`add ds1 07A19`**. Press **Enter**.

   The system displays the DS1 Circuit Pack screen. You must enter a specific port address for the circuit pack.

2. In the **Name** field, type **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, type **1.544**.

   This is the standard for T1 lines.

4. In the **Line Coding** field, type **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, type **esf**.

   Avaya recommends you use **esf** whenever your service provider supports it.

6. In the **Signaling Mode** field, type **robbed-bit**.
7. In the **Interface Companding** field, type **mulaw**.

   This is the standard for T1 lines in North America.
8. Press **Enter** to save your changes.

More information

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.

Matching field settings on different screens

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
Interface	Signaling Group
Interconnect	Tone Generation
Country Protocol	Signaling Group Tone Generation

1. See Avaya Aura™ *Communication Manager Screen Reference*, 03-602878

Specific combinations of settings for some of these fields are shown below.

ITC, Bit Rate, and Line Coding

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 corresponding Group Type entries.

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**

Related topics

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.

Adding trunks to a trunk group

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.

Before you start

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.

Instructions

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.

To assign trunks to trunk group 5:

1. Type **`change trunk-group 5`**. Press **Enter**.
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, type **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, type **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, type **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, type **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. Press **Enter** to save your changes.

Removing trunk groups

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.

Instructions

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.

To remove trunk group 5:

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.

   Remember to press **Enter** to save your changes.

3. In the Group Member Assignments screen for trunk group 5, remove all member trunks from the group.

   See Adding trunks to a trunk group on page 420 for instructions.

4. Type **`remove trunk-group 5`**. Press **Enter**.

   The system displays the Trunk Group screen.

5. Press **Enter** to remove the trunk group.

Resetting trunks

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.

To reset a trunk group:

1. Type **`busyout trunk n`**, where ***n*** is the number of the trunk group.
2. Type **`release trunk n`**.

   The trunk group is reset. (Example: **`busyout trunk 43`** followed by **`release trunk 43`**.)

To reset a trunk member:

1. Type **`busyout trunk n/x`**, where ***n*** is the number of the trunk, and ***x*** is the trunk group member.

2. Type **`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`**.)

Inserting and absorbing digits

Use this procedure 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.

Instructions

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:

1. Type **`change trunk-group 5`**. Press **Enter**.

   The system displays the Trunk Group screen.

2. In the **Digit Treatment** field, type **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, type **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, type **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. Press **Enter** to save your changes.

If your service provider sends 7 digits but you only need 5, you need to absorb the first 2 digits in the digit string. To absorb digits:

1. Type **`change trunk-group 5`**. Press **Enter**.

   The system displays the Trunk Group screen.

2. In the **Digit Treatment** field, type **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, type **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, type **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. Press **Enter** to save your changes.

Related topics

See Adding a DID trunk group on page 410 for instructions on administering a DID trunk group.

See Adding a Tie or Access trunk group on page 414 for instructions on administering a tie trunk group.

Administering trunks for Listed Directory Numbers

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.

Instructions

As an example, let us say that one attendant group answers calls for 3 different businesses, each with its own listed directory number:

- Company A — 855-2020
- Company B — 855-1000

- 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:

1. Type **`change listed-directory-numbers`**. Press **Enter**.

   The system displays the **Listed Directory Numbers** screen.

2. In the **Ext 1** field, type **2020**.

   This is the LDN for Company A.

3. In the **Name** field, type **Company A**.

   This name appears on the console display so the attendant knows which business the call is for and how to answer it.

4. Repeat steps 2 and 3 for the other two businesses.

   You can enter up to 20 different listed directory numbers on this screen.

5. Press **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 screen 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.

Related topics

See Listed Directory Numbers in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for detailed information about this feature.

Administering Answer Detection

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.

Before you start

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.

Instructions

As an example, we will administer trunk group 5 for both types of answer detection.

To administer trunk group 5 for answer supervision from the network:

1. On the Trunk Group screen for group 5, type **y** in the **Receive Answer Supervision** field.
2. Press **Enter** to save your change.

Now we will administer answer supervision by timeout. We'll set the timer to 15 seconds. To administer trunk group 5 for answer supervision by timeout:

1. On the Trunk Group screen for group 5, type **15** in the **Answer Supervision Timeout** field.
2. Press **Enter** to save your change.

Related topics

See Answer Detection in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205*,* for detailed information about this feature.

Administering ISDN trunk groups

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**.

Hardware requirements

ISDN-BRI interfaces are supported by the TN2185 Trunk-side BRI circuit pack (for implementing the user side of the BRI interface) and by the TN556B or TN556C ISDN-BRI Line circuit pack or the TN2198 ISDN BRI (U-LT) Line circuit pack (for the network side of the BRI interface). 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	**All**
DS1 Circuit Pack screen (if using ISDN-PRI interfaces)	**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

For proper transmission of QSIG name data for display, administer the following settings:

- Trunk Group screen
  - **Group Type**: **ISDN**
  - **Character Set for QSIG Names**: **iso8859-1**
  - **Outgoing Display**: **y**
  - **Send Calling Number**: **y**
  - **Send Name**: **y**
- Signaling Group screen
  - **Supplementary Service Protocol**: **b**
- System-Parameters Country-Options screen
  - **Display Character Set**: **Roman**

Chapter 13: 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.

Getting Started with the VAL or G700 Virtual VAL

Before you can use the capabilities of the VAL or G700 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*
	1 of 3

Task	Information source
Installing v VAL for a G700 Media Gateway using the Media-Gateway screen and the **`enable announcement`** command Administering IP Connections Adding IP Routes Testing the IP Connections **Note:** G700 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.	Each G700 Media Gateway that will be used to provide announcements through the embedded VAL circuitry on the Gateway processor circuit pack must be assigned on 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 G700 Media Gateway first must be assigned on the Media-Gateway screen so as to be used for gateway announcements. Each G700 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 G700 Media Gateway must have the **V9** field assigned to **gateway-announcements** on the Media-Gateway screen before the G700 embedded VAL (v VAL) can be enabled. Then the G700 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 G700 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*
	2 of 3

Task	Information source
Viewing announcement usage measurements (**`list measurements announcement`** command)	*Avaya Aura™ Communication Manager Reports* and *Avaya Aura™ Communication 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).
	3 of 3

Chapter 14: Managing Group Communications

Setting up Voice Paging Over Loudspeakers

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.

Before you start

Your server running Communication Manager must have 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.

Instructions

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.

1. Type **`change paging loudspeaker`**. Press **Enter**.

   The system displays the Loudspeaker Paging screen.

2. In the **Voice Paging Timeout** field, type **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**, type **01C0501**.

   Use this field to assign a port on an auxiliary trunk circuit pack to this zone.

4. In the **Voice Paging — TAC** field type **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 type **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, type **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, type **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. Press **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.

Fixing problems

Problem	Possible causes	Solutions
Users report that they can't page.	The attendant has taken 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 calls are forwarded to.

More information

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.

Related topics

See Paging Over Speakerphones on page 442 for another way to let users page.

See Loudspeaker Paging in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205, for detailed information on voice paging over loudspeakers.

Setting up Chime Paging Over Loudspeakers

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.

Before you start

Your server running Communication Manager must have 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.

Instructions

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.

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.

1. Type **`change paging loudspeaker`**. Press **Enter**.

   The system displays the Loudspeaker Paging screen.

2. In the **Code Calling Playing Cycles** field, type **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**, type **01A0301**.

   Use this field to assign a port on an auxiliary trunk circuit pack to this zone.

4. In the **Code Calling — TAC** field type **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 type **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, type **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, type **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. Press **Enter** to save your changes.

To assign chime codes to individual extensions:

1. Type **`change paging code-calling-ids`**. Press **Enter**.

   The system displays the **Code Calling IDs** screen.

2. Type 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. Press **Enter** to save your changes.

Fixing problems

Problem	Possible causes	Solutions
Users report that they can't page.	The attendant has taken control of the trunk group.	Deactivate attendant control.

More information

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.

Related Topics

See Paging Over Speakerphones below for another way to let users page.

See Loudpeaker Paging in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205, for detailed information on chime paging over loudspeakers.

Paging Over Speakerphones

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.

Before you start

You must have DCP set speakerphones or IP set speakerphones.

Instructions

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.

1. Type **`add group-page 1`**. Press **Enter**.

   The system displays the Group Paging Using Speakerphone screen.

2. In the **Group Extension** field, type **3210**.

   This field assigns the extension users dial to page the members of this group.

3. In the **Group Name** field, type **Sales staff**.

   This name appears on callers' telephone displays when they page the group.

4. In the **COR** field, type **5**.

   Any user who wants to page this group must have permission to call COR 5.

5. In the **Ext** field in row 1, type **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. Press **Enter** to save your changes.

Fixing problems

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.
	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.

More information

- 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.

Related topics

See Group Paging in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205, for detailed information on paging over speakerphones.

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.

Before you start

Before you administer whisper paging:

- Your Communication Manager server must have 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.
- Users must have 6400-, 7400-, 8400-, or 9400-series DCP (digital) telephones.

Instructions

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.

Related topics

See Whisper Paging in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205, for detailed information on whisper paging.

Using Telephones as Intercoms

Use this procedure 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.

Instructions

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.

In this example, we'll create intercom group 1 and add extensions 2010 to 2014.

1. Type **`add intercom-group 1`**. Press **Enter**.

   The system displays the Intercom Group screen.

2. Type **1** in the **Length of Dial Code** field.

   Dial codes can be 1 or 2 digits long.

3. On row 1, type **2010** in the **Ext** field.

4. On row 1, type **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. Press **Enter** to save your changes.

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.

To set up automatic intercom between extensions 2010 and 2011:

1. Type **`change station 2010`**. Press **Enter**.

   The system displays the **Station** screen.
2. Move to the page with the **BUTTON ASSIGNMENTS** fields.
3. In **BUTTON ASSIGNMENTS** field **4**, type **auto-icom**. Press **Tab**.

   The **Grp** and **DC** fields appear.
4. In the **Grp** field, type **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, type **2**.

   This is the dial code for extension 2011, the destination extension.
6. Press **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.

Related topics

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.

Setting up Automatic Answer Intercom Calls

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

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. To do so, complete the following steps:

1. Type **`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. Press **Enter** to save your changes.

Observing Calls

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.

Before you start

On the System Parameter Customer-Options screen, verify that the:

- **Service Observing (Basic)** field is **y**.

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.

Instructions

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.

To set up service observing:

1. Set the observer's class of restriction to permit service observing:
   a. In the Class of Restriction screen for COR 5, type **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. Type **y** in the field for class of restriction 10.

2. In the Class of Restriction screen for COR 10, type **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, type **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.

In order 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.

Note:
Best practices for service observing:

- 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.
- 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.
- 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.
- 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.

Related topics

See Service Observing in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205, for detailed information on service observing.

Chapter 15: 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 CM 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

Administering Data Call Setup

For data-terminal dialing:

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.

For telephone dialing:

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 Manager Screen 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.

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 6: 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)

The following call-progress messages and their meanings are provided for DCP and ISDN-BRI modules.

Table 7: 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.
INCOMING CALL	DCP, BRI	Equivalent to ringing.

1 of 2

Table 7: Call-progress messages (continued)

Message	Application	Meaning
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.
DISCONNECTE D	DCP, BRI	Call is disconnected.
WAIT	DCP, BRI	Normal processing continues.
WAIT, XX IN QUEUE	DCP	Call is in a local hunt-group queue.
		2 of 2

DCP data modules

Data-terminal dialing

DCP data-terminal dialing allows a user to set up and disconnect data calls directly from a data terminal as follows.

1. At the **DIAL**: prompt, the user types the data number. The message **RINGING** displays.
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.

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

Data-terminal dialing

A user can set up and disconnect data calls directly from a data terminal without using a telephone as follows:

1. The user presses **Enter** a few times. If the CMD: prompt does not appear, the user presses **Break A + T** at the same time, and then presses **Enter**.
2. At the **CMD**: prompt, the user types and presses **Enter**.

3. To disconnect, the user enters +++. At the CMD: prompt, the user types **end** and presses **Enter**.

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

- A BRI telephone cannot call a data terminal, and a data terminal cannot call a BRI telephone.

Interactions

- 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

To set up alphanumeric dialing:

1. On the Alphanumeric Dialing Table screen, administer the **Alpha-name** and **Mapped String** fields.

Considerations

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.

Administering Data Hotline

To administer a data hotline:

1. 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.
2. On the Station screen, administer the following fields.

- Abbreviated Dialing List
- Special Dialing Option
- Hot Line Destination

3. 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

- 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

To administer data privacy:

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

- 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

- 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

To administer default dialing:

1. 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.
2. 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

To administer data restriction:

1. On the Station screen, set the **Data Restriction** field to **y**.
2. Choose one of the following trunk groups and set the **Data Restriction** field to **y**.
   - 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 - 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

To administer data-only off-premises extensions:

1. 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.

Consideration

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

- 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 CM 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 Connection

An Administered Connection (AC) is a connection between two access or data endpoints. Communication Manager automatically establishes and maintains the connection based on the attributes you administer. ACs provides the following capabilities.

- Support of both permanent and scheduled connections
- Auto Restoration (preserving the active session) for connections routed over Software Defined Data Network (SDDN) trunks
- Administrable retry interval (from 1 to 60 minutes) per AC
- Administrable alarm strategy per AC
- Establishment/retry/auto restoration order based on administered priority

Detailed description

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

Access endpoints are non-signaling trunk ports. They neither generate signaling to the far-end of the trunk nor respond to signaling from the far-end. Designate an access endpoint as the originating endpoint or destination endpoint in an AC.

Typical AC applications

The following are typical AC applications:

- A local data endpoint connection to a local or remote-access endpoint. Examples: an MPDM ACCUNET digital service connecting to SDDN via an ISDN trunk-group DS1 port; an MPDM ACCUNET digital service connecting to an ACCUNET Switched 56 Service via a DS1 port.
- A local-access endpoint connecting to a local or remote-access endpoint. Examples: a DSO cross-connect and a 4-wire leased-line modem to a 4-wire modem connection via an analog tie trunk.
- A local data endpoint connecting to a local or remote data endpoint such as a connection between two 3270 data modules.

Note:
The following guidelines do not include AAR and ARS, or GRS administration information for routing AC calls over trunk groups. See the respective feature elsewhere in this book for that information.

Establishing Administered Connections

The originating server or Avaya S8XXX Server attempts to establish an AC only if one of the following conditions exist:

- AC is active.
- AC is due to be active (either a permanent AC or time-of-day requirements are satisfied if it is a scheduled AC).
- Originating endpoint is in 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 desired 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, Communication Manager arranges the connections in order of priority.

AC attempts can fail for the following reasons:

- Resources are unavailable to route to the destination.
- A required conversion resource is not available.
- Access is denied by class of restriction (COR), facilities restriction level (FRL), or bearer capability class (BCC). Or, an attempt is made to route voice-band-data over SDDN trunks in the public switch network.
- Destination address is incorrect.
- Destination endpoint is busy.
- Other network or signaling failures occur.

In the event of a failure, an error is entered into the error log, which generates an alarm, if it is warranted by your alarming strategy. You can display AC failures via the **`status-administered connection`** command.

As long as an AC is due to be active, the originating server continues to establish an AC unless the attempt fails because of an administrative error (for example, a wrong number) or service-blocking condition (for example, outgoing calls barred).

- The frequency with which failed attempts are retried is determined by the administered retry interval (1 to 60 minutes) for each AC.
- Retries are made after the retry interval has elapsed regardless of the restorable attribute of the AC.
- ACs are retried in priority order.
- When you change the time of day on Communication Manager, an attempt is made to establish all ACs in the waiting-for-retry state.

Dropping Administered Connections

An AC remains active until one of the following 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. This could be because of user action (in the case of a data endpoint), maintenance activity resulting 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 (for example, facility failure) occurs between the endpoints.

If an AC drops because it was disabled/removed or is no longer due to be active, no action is taken. If an AC drops because of changed AC attributes, an immediate attempt is made to establish the connection with the changed attributes if it is still due to be active. Existing entries in the error/alarm log are resolved if they no longer apply. If handshake failure resulted in the dropping of the connection, in the case of an AC involving at least one data endpoint, no action is taken for that AC until the **`change administered-connection`** command is executed.

Administered Connections failure: Auto Restoration and Fast Retry

When an active AC drops prematurely, you must invoke either auto restoration or fast retry to determine whether auto restoration is attempted for an active AC.

If you option AC for auto restoration 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 allowing the active session to be maintained, AC also provides a high level of security by prohibiting other connections from intervening in active sessions. Auto restoration generally completes before the 60-second endpoint holdover interval. If auto restoration is successful, the call might be maintained (no guarantee). 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 reflected by the *restored* state on the status Administered Connection screen. Although the restoration was successful, the data session might not have been preserved.

If auto restoration is not active or if the AC is not routed over SDDN trunks, Communication Manager immediately attempts to reestablish the connection (fast retry). Communication Manager also attempts a retry if the originating endpoint initiated the drop. With fast retry, connections are not maintained on both ends. Fast Retry is not attempted for an AC that was last established via fast retry, unless the AC is active for at least two minutes.

If auto restoration 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 due to be active.

Administering Administered Connections

To administer administered connections:

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)
- X.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)

1. On the DS1 Circuit Pack screen, administer all fields. Use with switch node carriers.
2. On the Access Endpoint screen, administer all fields.
3. On the Trunk Group screen, choose one of the following trunk groups and administer all fields.
   - ISDN-BRI
   - ISDN-PRI
   - Tie
4. On the Class of Restriction screen, administer all fields.
5. On the Class of Service screen, administer all fields.
6. 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.
7. On the Administered Connection screen, administer all fields.
8. On the Station screen, assign one button as ac-alarm.
9. On the Attendant Console screen, assign one button as ac-alarm.

Interactions

- 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 Modem Pooling

For Integrated modem poolings:

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.

For Combined modem poolings:

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

- 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.

Interactions

- Call Detail Recording

  Data call CDR records the use of modem pools on trunk calls.
- Data Call Setup

  Data calls to or from a TDM cannot use Modem Pooling.
- Data Privacy and Data Restriction

  The insertion of a modem pool does not turn off Data Privacy or Data Restriction.
- Data-Only Off-Premises Extensions

  Calls to or from a Data-Only Off-Premises Extension cannot use Modem Pooling, when this type of digital-data endpoint uses a TDM.
- DMI Trunks

  If you place a data call from a local analog-data endpoint to a DMI trunk, you must dial the data-origination access code to obtain a modem. Data calls on DMI trunks to local analog-data endpoints automatically obtain modems.
- DS1 Tie Trunk Service

  Connect modems used for Modem Pooling to AVD DS1 tie trunks via Data Terminal Dialing or by dialing the feature-access code for data origination.

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 476) 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 53: DCP PC interface configuration (Group 1)

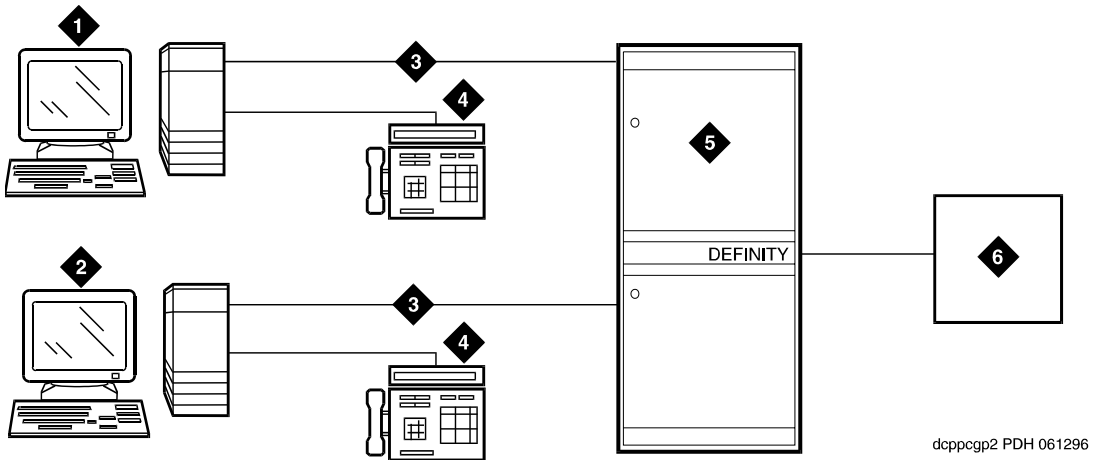


Figure notes:

1. IBM-compatible PC with DCP Interface card
2. IBM-compatible PC with DCP Interface card
3. DCP
4. DCP telephone
5. Avaya (Digital Line, Digital Line (16-DCP-2-Wire), or Digital Line (24-DCP-2-wire) circuit pack)
6. 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 Figure 54) 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 54: ISDN—BRI PC interface configuration (Group 2)

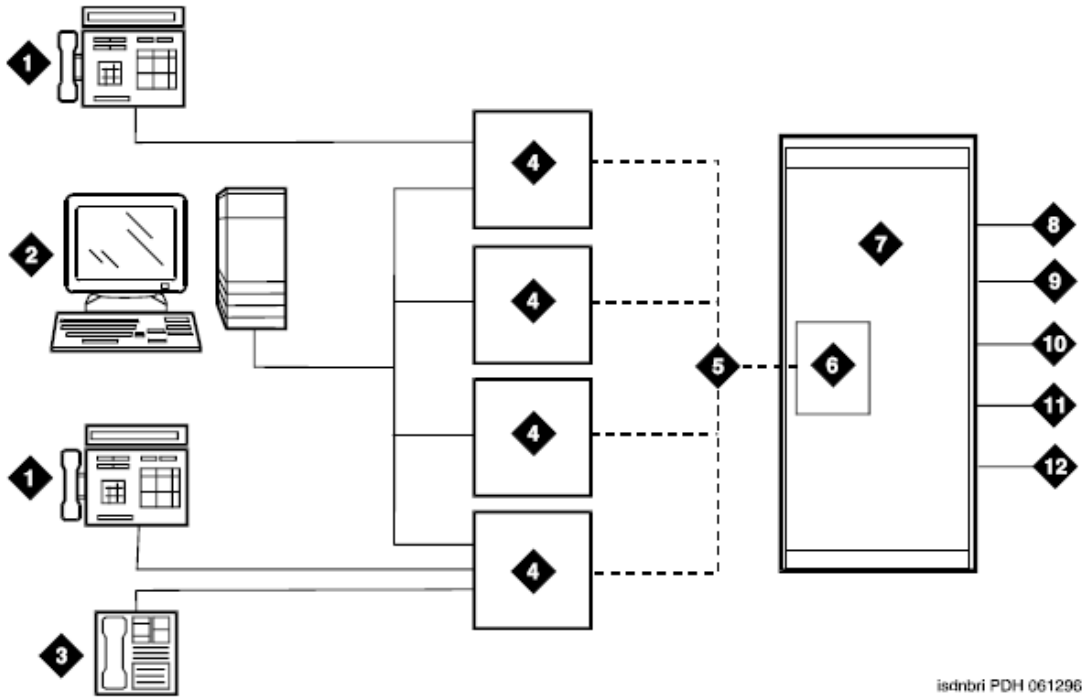


Figure notes:

1. ISDN telephone
2. PC with application
3. Handset or Headset
4. BRI Interface card
5. 2B + D
6. ISDN Line (12-BRI-S-NT) circuit pack)
7. Avaya S8XXX Server
8. PRI trunks
9. BRI stations
10. Interworking
11. DMI
12. 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.

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

To administer a PC interface:

1. On the Station screen, set the **Type** field to **pc**.

Considerations

- 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

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.

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

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).

Typical uses

A typical video application uses an ISDN-PRI interface to DS0 1 through 6 of the line-side facility. See Figure 55: Wideband Switching Video Application on page 481.

Figure 55: Wideband Switching Video Application

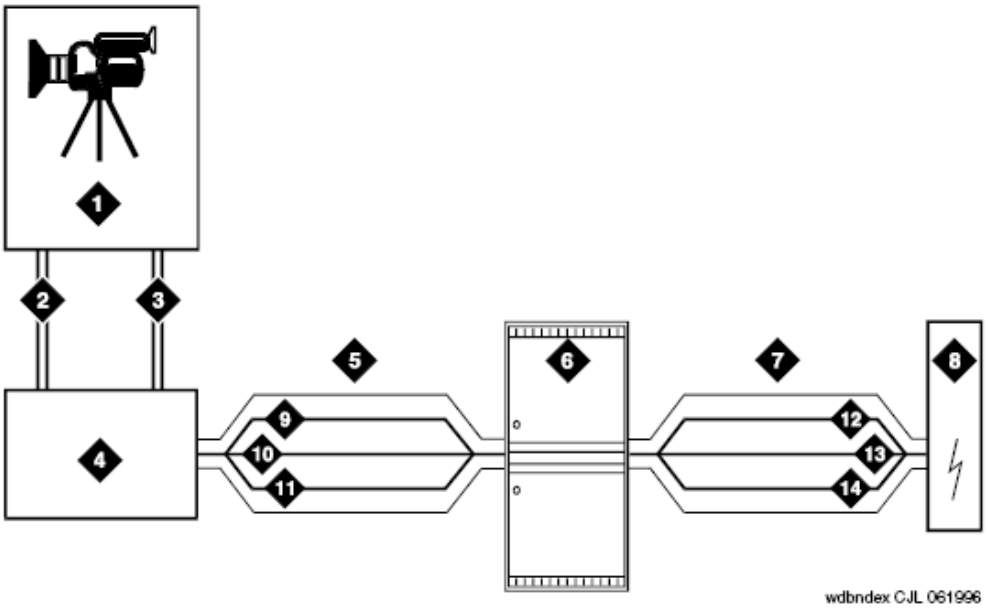


Figure notes:

1. Video application
2. Port 1
3. Port 2
4. ISDN terminal adaptor
5. Line-side ISDN-PRI
6. Avaya S8XXX Server
7. ISDN trunk
8. Network
9. DS0 24 D-channel
10. DS0 23 unused
11. DS0 1 to 6 wideband
12. DS0 24 D-channel
13. DS0 7 to 23 narrow bands
14. DS0 1 to 6 wideband

Endpoint applications

An endpoint application is the origination or destination of a wideband call. Endpoint application can be any number of data applications based on the customer's particular needs.

ISDN-PRI terminal adapters

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 (to the endpoint) applications and outgoing calls.

Line-side (T1 or E1) ISDN-PRI facility

A line-side ISDN-PRI (T1 or E1) facility is comprised of a group of DS0s (24 for a T1 facility and 32 for an E1 facility). 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 bi-directionally across the facility between the server and the ISDN-PRI terminal adapter.

PRI-endpoints

A PRI-endpoint (PE) is a combination of DS0 B-channels on a line-side ISDN-PRI facility that has been assigned an extension.

A PRI-endpoint can support calls of lower bandwidth. In other words, a PE having a width 6 (six DS0s) can handle a call of one channel (64 Kbps) up to an including 6 channels. For example, an endpoint application connected to a PE defined as using B-channels 1 through 6 of an ISDN-PRI facility could originate a call using B-channels 1, 3, and 5 successfully. If the PE has been administered to use flexible channel allocation, the algorithm for offering a call to the PE starts from the first DS0 administered to the PE. Since only one active call is permitted on a PE, contiguous B-channels always are selected unless one or more B-channels are not in service.

One facility can support multiple separate and distinct PRI-endpoints (several extensions) within a single facility. Non-overlapping contiguous sets of DS0s (B-channels) are associated with each PE.

Universal digital signaling level 1 circuit pack

The UDS1 circuit pack is the interface for line-side and network facilities carrying wideband calls.

Non-signaling configuration

Wideband also can support configurations using non-signaling (non-ISDN-PRI) line-side T1 or E1 connections. The endpoints are the same as those defined for configurations with signaling.

Data service unit/channel service unit

This unit simply 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

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.

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

Data backup connection

Using wideband for data transmission backup provides customers with alternate transmission paths for critical data in the event of primary transmission path failure.

Scheduled batch processing

Scheduled batch processing applications are used for periodic database updates (for example, retail inventory) or distributions (for example, 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. In addition, wideband allows the dedicated-access bandwidth for busy-hour switching traffic to be used for these applications after business hours; 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 originating from this application.

Primary data connectivity

Permanent data connections (those always active during business hours), such as interconnections between LANs, are well suited for Communication Manager when ISDN-PRI endpoints are used. The ISDN end-to-end monitoring and the endpoint's ability to react to failures provide for critical data availability needs. With ISDN, endpoints can detect network failures and initiate backup connections through the server running Communication Manager; ISDN endpoints can also establish additional calls when extra bandwidth is needed.

Any failures not automatically restored by Communication Manager are signaled to the endpoint application, which can initiate backup data connections over the same PRI endpoint. Communication Manager routes the backup data connections over alternate facilities if necessary.

Networking

All of the wideband networking is over ISDN-PRI facilities (and the emulation of them by ATM-CES) but might connect to a variety of networks, other domestic interexchange carriers' services, private line, RBOC services, and services in other countries.

ISDN-PRI trunk groups and channel allocation

Only ISDN-PRI trunks (and the emulation of them by ATM-CES) support wideband calls to the network. Wideband's bandwidth requirements have necessitated modification of the algorithms by which trunks look for idle channels. The following section describes the search methods and their relationship to the available wideband data services.

Facility lists

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

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

Since H12 is 1,920 Kbps which is comprised of 30 B-channels, a 1,920-kbps call can only be carried 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 always is carried on B-channels 1 to 15 and 17 to 31 on an E1 facility (as shown in the following table). When offered any other call (other than a 1,536-kbps call), the algorithm behaves as it does when H11 is optioned.

		DS0s Comprising Each Channel	
Facility	**ISDN Interface**	**H11**	**H12**
T1 T1	23B + D 24B (NFAS)	- 1-24	- -
E1 E1	30B + D 31B (NFAS)	1-15, 17-25 1-15, 17-25	1-15, 17-31 1-15, 17-31

H0

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

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.

Glare and blocking

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.

Blocking prevention

Blocking occurs when insufficient B-channels required to make a call are available. Narrowband calls require only one channel so blocking is less likely than with wideband calls which require multiple B-channels. Blocking also occurs for wideband calls when bandwidth is not available in the appropriate format (that is, fixed, floating, or flexible).

To reduce blocking, Communication Manager selects trunks for both wideband and narrowband calls to maximize 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 to minimize blocking depends on the channel type. The chances for blocking are reduced if you use a flexible algorithm, assuming it is supported on the other end.

Channel Type	Blocking Minimization Strategy
H0	Preserve idle quadrants
H11	Preserve idle facilities
H12	Preserve idle facilities
Flexible NxDS0	Preserve idle facilities
Floating NxDS0	Preserve idle facilities as first priority

Administering Wideband Switching

Before you start, you need a DS1 Converter circuit pack.

To administer wideband switching:

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 with non-ISDN-PRI equipment, you can use an ISDN-PRI terminal adapter.

Interactions

- Administered Connections

  Provides call initiation for WAEs. All Administered Connections that originate from WAEs use the entire bandwidth administered for WAE. The destination of an Administered Connection can be a PRI endpoint.

- Automatic Circuit Assurance

  Treats wideband calls as logical single-trunk calls so that a single ACA-referral call is made if an ACA-referral call is required. The call is referred to the lowest B-channel associated with the wideband call.

- Call Coverage

  A wideband endpoint extension cannot be administered as a coverage point in a call-coverage path.

- Call Detail Recording

  When CDR is active for the trunk group, all wideband calls generate CDR records. The feature flag indicates a data call and CDR records contain bandwidth and BCC.

- Call Forwarding

  You must block Call Forwarding through Class of Service.

- Call Management System and Basic Call Management System

  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 can use a vector-directory number (VDN) when dialing. 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.

  Call Vectoring is used by certain applications. When an incoming wideband call hunts for an available wideband endpoint, the call can route to a VDN, that sends the call to the first available PRI endpoint.

- Class of Restriction

  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 is turned off for wideband endpoints.

- 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

  You can use Facility Test Calls to perform loop-back testing of the wideband call facility.

- Generalized Route Selection

  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 can support other BCCs to allow different call types to share the same trunk group.

- CO Trunk (TTC - Japan) Circuit Pack

  This 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).

For a simple ASAI configuration example, see Figure 56.

Figure 56: ASAI Switch Interface Link — BRI Transport

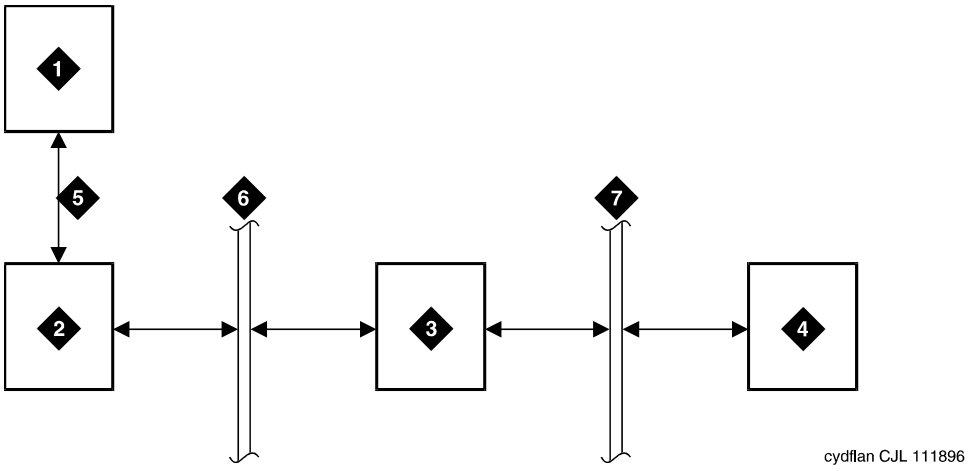


Figure notes:

1. ASAI adjunct
2. ISDN Line circuit pack
3. Packet Controller circuit pack
4. Switch processing element (SPE)
5. ISDN-BRI
6. Packet bus
7. Memory bus

ASAI Capabilities

For information concerning the types of associations over which various event reports can be sent, see *Avaya Communication Manager ASAI Technical Reference*, 555-230-220.

Considerations

- If your system has an expansion cabinet (with or without duplication), ASAI resources should reside on the system's Processor Cabinet.

Interactions

See *Avaya Communication Manager ASAI Technical Reference*, 555-230-220.

Setting up CallVisor ASAI

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.

Before you start

- On the System Parameters Customer-Options (Optional Features) screen, verify 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.

Instructions

To set up CallVisor ASAI:

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 16: Administering Avaya Servers

This chapter describes how to administer an Avaya S8xxx Server and an Avaya G700 Media Gateway. 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 and of the Avaya P330 switches is also recommended.

Overview

To set up and maintain your Avaya S8xxx Server with a G700 Media Gateway, you need to administer:

- the G700 Media Gateway and its internal processors, typically using the P330 Device Manager Web-based tool or a command-line interface (CLI)
- the Avaya S8xxx Server using the Server Web Interface
- call-processing features using Communication Manager

Administering the G700 Media Gateway

The hardware elements of the G700 Media Gateway are summarized in this section. For details on any of these hardware components or on different configurations, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

G700 Media Gateway physical design

The G700 Media Gateway is a19-inch, rack-mount design similar to other Avaya P330 hardware. The media gateway can be a member of a P330 stack of Layer 2 or 3 devices, reside in a stack of other media gateways, or operate as a standalone unit. Figure 57 shows the front of the media gateway.

Figure 57: The G700 Media Gateway (front view)

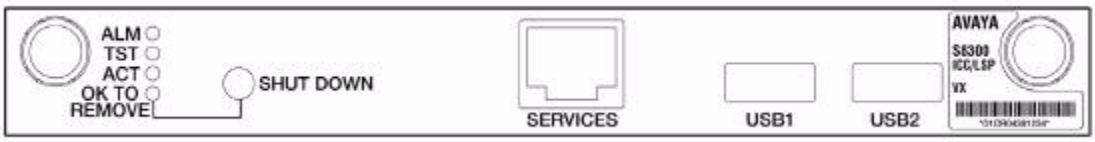
Key components of the G700 Media Gateway include:

1. LED Status Panel (top left) for the media gateway
2. S8300 Server slot (V1). The G700 Media Gateway does not have an S8300 Server in its basic configuration.
3. P330 Expansion slot (bottom left) for adding modules such as a 16-port Ethernet expansion module, fiber interfaces, ATM access or WAN access
4. Dual 10/100Base-T Ethernet Ports for connection to the corporate LAN (bottom center of chassis)
5. Up to three additional media modules in slots V2 to V4 on the right side of the chassis (slots are numbered from top to bottom)
6. 8-Pin RS-232 Serial Port (Console) for direct-connect P330 stack processor administration (typically done by Services personnel)

S8300 Server faceplate

(For S8300 Servers) Figure 58 shows the faceplate of the S8300 Server.

Figure 58: S8300 Server faceplate



The faceplate of the S8300 Server has the following components:

- The LED array on the left indicates when the S8300 is active and when it is safe to power it down. The green LED indicates that Communication Manager is running.

- A Shut Down button can be used to shut down the server (the S8300 can also be shut down and restarted using software commands).
- A Services Ethernet interface provides a direct connection to a laptop computer connected with a crossover cable. Normally only Services technicians use this interface; most ongoing S8300 administration is done using the Ethernet connection to the corporate LAN on the media gateway.
- One of the two USB connections can be used to attach an external modem, primarily used to report alarms to a Services support agency.
- The label on the right provides identification information for the S8300 Server.

G700 Media module description

(For S8300 Servers) The four slots on the G700 Media Gateway are populated with media modules according to the needs at your site. Up to four slots can be filled as follows:

- The S8300 Server is a special type of media module that hosts the call-processing (telephony) software. If present, the S8300 is installed in slot one (V1); only one can be installed per media gateway. The S8300 can act as a primary call controller for the system, or one or more S8300s can be configured to provide standby service for a primary call controller if needed. See Configuring the Local Survivable Processor on page 496 for details.
- The other media module slots are filled as needed to meet the call-processing needs at your site. Media modules can be mixed and matched. Table 1 lists the administrative name and port capacities for the media modules that can be installed in a G700 Media Gateway.

Table 8: Media Module names and port capacities

Media module type	Administration name	Number of ports
Analog Line/Trunk	analog	8
DCP Telephone	dcp	8
T1/E1	ds1	24/32 (T1=24 in robbed-bit signalling mode and E1=32 for 1 control, 1 signal and 30 voice)
VoIP	voip	N/A
S8300 Server	icc	N/A
MM270	bri	8

Configuring the Local Survivable Processor

An Avaya S8xxx Server can be configured either as the primary call-processing controller, or as a Local Survivable Processor (LSP). An LSP 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 LSP server; it is set up to operate as a primary or standby LSP 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 G700 Media Gateway, the media gateway retains its last status until the Link Loss Delay Timer (LLDT) expires. (The default for the LLDT is 5 seconds, 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 G700 loses contact with the Avaya S8xxx Server, the media gateway first tries to reconnect for a period of one minute. If this fails, then the G700 then tries to connect with another server in its controller list. If the primary server was a LSP, 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 an LSP 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 (LSP) 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.

- When the primary server is available again, it will begin handling call processing. However, those endpoints that are now using the standby server will continue to do so until the standby unit is rebooted.
- 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 LSP will be dropped when the reboot occurs (the change back to the primary server is not call preserving).
- With LSP functionality, there is full functionality and feature support.

Using Device Manager to administer G700 Media Gateway components

Device Manager, also known as the P330 Embedded Web Manager, provides a browser-based graphical user interface (GUI) to assist you with ongoing media gateway administration.

Device Manager allows you to:

- View the status of different devices on the network.
- Configure or modify devices including Virtual LAN (VLAN) groupings, port mirroring, and Simple Network Management Protocol (SNMP) traps.

Accessing Device Manager from a Web browser

To access the P330 Device Manager from a Web browser:

1. Open a compatible Web browser on your computer. Microsoft Internet Explorer versions 6.0 and 7.0 are supported. The Java Plug-in 1.3.1_02 is required.
2. In the **Address (or Location)** field of your browser, type the IP address of the P330 stack.
3. Log in as prompted.
   - The default user name is: **root**
   - The default password for read-write access is: **root**

   Note:
   You should change the default passwords after you log in, if they have not already been changed. The passwords apply to all logins for these devices, whether accessed through Device Manager or a CLI.
4. The Welcome screen is displayed. Proceed with P330 and media gateway device administration.

Accessing Device Manager through Network Management Console with VoIP SystemView

You can alternatively launch the P330 Device Manager from the Avaya Network Management Console with VoIP SystemView. This optional product is a complete Network Management System (NMS). Services include:

- viewing all network devices by type, subnet, or customized groupings
- logging and viewing SNMP traps and events
- launching and managing other applications including Avaya Site Administration

Contact your Avaya representative to obtain a copy of this program if desired.

Administering the command line interface

Instead of using Device Manager, you can access the server's command line interface using an SSH client, like PuTTY, and an IP address of 192.11.13.6., or use the serial interface on the front of the chassis to establish a direct connection to the P330 stack processor.

- 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 to Avaya's Initialization and Administration System (INADS) or another services support agency over the server's optional modem interface or through SNMP notifications. Either method, both, or no alarm-reporting method might be used at a given site.

Administering the Avaya S8xxx Server

The Avaya S8xxx Server contains the call-processing software of Communication Manager, and controls 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.
- Checking server and process status.
- Administering network features for the server such as SNMP service, enabling or disabling the modem (if used), enabling FTP services, and installing license and authentication files.
- Installing new software and reconfiguring the server as needed.
- Performing routine diagnostics and troubleshooting such as viewing alarms and system logs, and running tests if needed.

Accessing the Avaya S8xxx Server Web Interface

Avaya S8xxx Server tasks are performed using the Server Web Interface. This browser-based server administration tool is an easy-to-use graphical user interface for performing the server administration tasks listed above. It contains an extensive help system that describes all Web screens and Avaya S8xxx Server procedures. This section covers highlights of Avaya S8xxx Server administration.

The Web Interface can be accessed through the corporate LAN connection to the G700 Media Gateway, or through the Services Ethernet interface on the front of the Avaya S8xxx Server connected to a laptop PC using a crossover cable. Details on how to configure a laptop for a direct connection are in the online help and in *Welcome to the Avaya S8300 Media Server and Avaya G700 Media Gateway*.

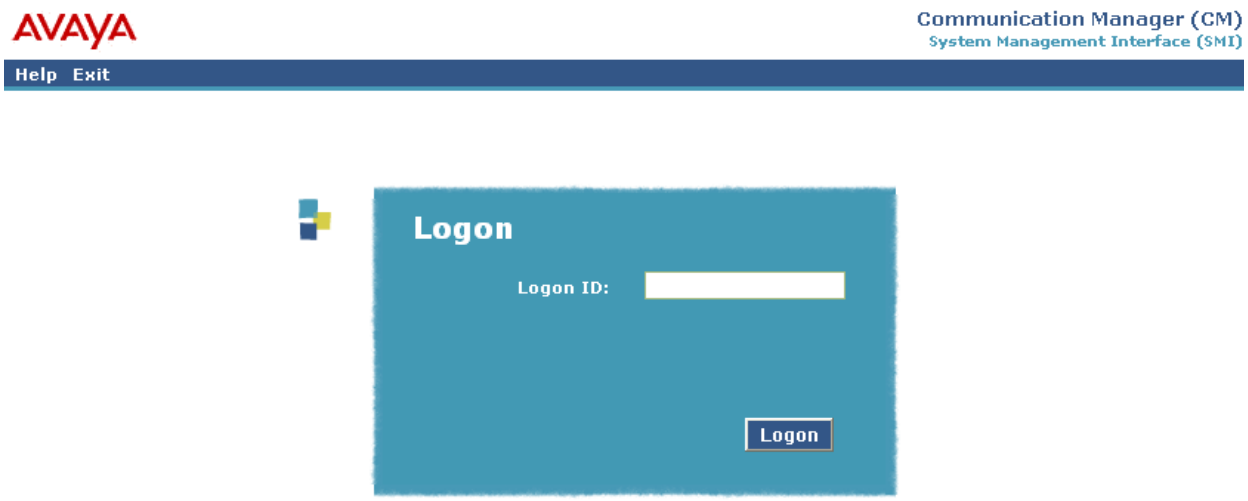
To access the Avaya S8xxx Server, you must log in as follows:

1. Open a compatible Internet browser on your computer. Currently only Microsoft Internet Explorer versions 6.0 and 7.0 are supported.
2. In the **Address (or Location)** field of your browser, type the IP address or name of the Avaya S8xxx Server. Press **Enter**.
   - LAN access by IP address. If you are logging into the administrative interface over the corporate local area network, you can type the Avaya S8xxx Server's unique IP address in standard dotted-decimal notation, such as http://192.152.254.201.
   - LAN access by server name. If the server has already been configured and if the corporate LAN includes a domain name service (DNS) server that has been administered with the servers' names, you can type the server's name into the address field instead of the IP address. Server names vary depending on local administration (such as http://media-server1.mycompany.com).
   - Laptop access by IP address. If you are logging in to the services Ethernet interface from a directly connected laptop, the IP address on the server is always **192.11.13.6**. The subnet mask is always **255.255.255.252**. New servers that have not yet been configured can only be accessed in this way. Server-name login is *not* available through the services interface because this connection is a closed (private) network with no DNS. The name and IP address of the Avaya S8xxx Server are specified during initial server configuration.

   Note:
   If your browser does not have a valid security certificate, you will see a warning screen and 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.

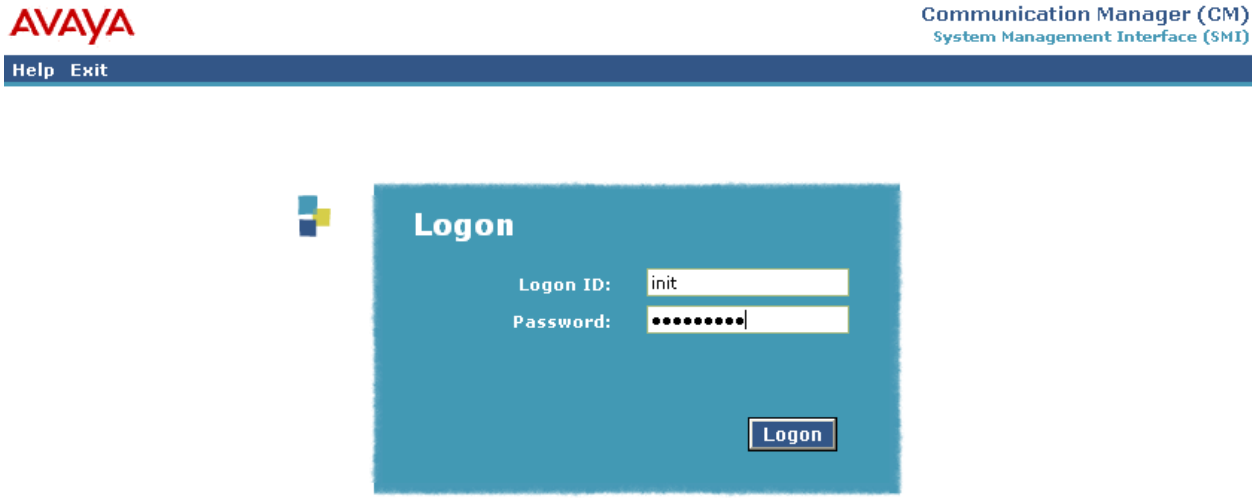
Figure 59: Communication Manager SMI Logon screen



3. In the **Logon ID** field, type your user name, such as **cust**. Remember that user names and passwords are case sensitive. Enter the login ID and confirmation information in upper or lower case as required. Click the **Logon** button or press **Enter**.

   The system redisplays the Logon screen with a **Password** field.

Figure 60: Communication Manager SMI Logon/Password screen

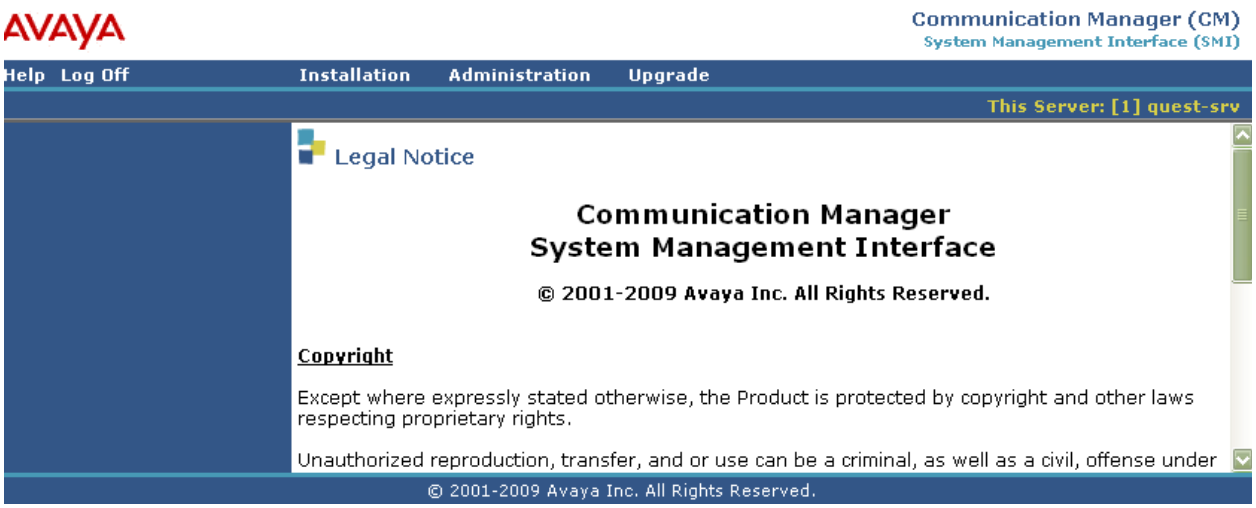


4. Type your password in the **Password** field, and click **Logon** or press **Enter**.

Note:
If your login is Access Security Gateway (ASG) protected, you will see an ASG challenge screen. Enter the correct response and click **Logon** or press **Enter**.he server matches your login information against authentication tables. If the server cannot recognize your user name or password, you receive an authentication failure message. Return to step 4. If you fail to enter the user name and login confirmation correctly 4 times within a few minutes, the Logon screen will block further attempts to log on for a while.

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

Figure 61: Communication Manager SMI home page



Accessing the Server Administration Interface

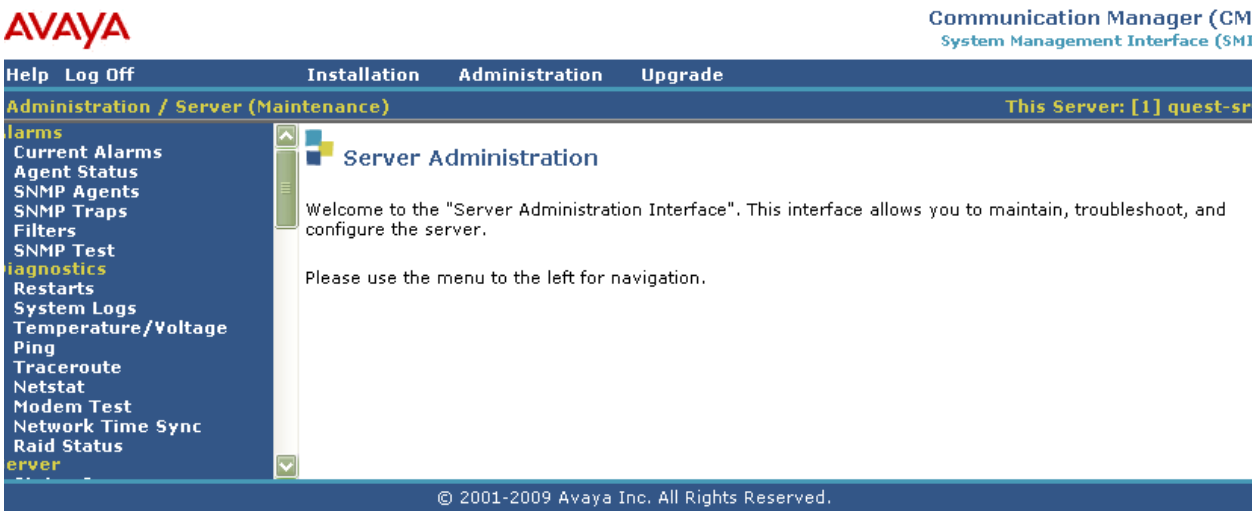
The Server Administration Interface allows you to maintain, troubleshoot, and configure the Avaya S8xxx Server.

To access the Server Administration Interface:

1. From the Communication Manager SMI home page (see Figure 61), on the **Administration** menu, click **Server (Maintenance)**.

   The system displays the Server Administration Interface home page.

Figure 62: Server Administration Interface home page



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.

Avaya S8xxx Server Web interface tasks

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

Backing up and restoring data

One of the most important tasks is to set up a schedule to routinely back up system data to a safe location. Because the S8300 Server does not include a media storage device for backup purposes, the data must be emailed or transferred using file transfer protocol (FTP) to another server or computer for backup. The S8700-Series Server has a local removable storage device.

The Web interface allows you to back up call-processing data (Communication Manager "translations"), server system data, and security files. Avaya recommends that you encrypt the backup files to keep this sensitive information secure.

Upgrading software and configuration

Occasionally you might need to install new software on the Avaya S8xxx Server. The new software (and a new license file if required) must be copied to the server using one of the methods listed in Copying files to the server on page 503. The software installation process uses wizard-like screens on the Web to guide you through the process.

You might also need to update your server configuration from time to time, and reverify it after a software upgrade. IP addresses for the server and its gateway to the corporate LAN, or for the optional UPS unit, DNS servers, and modem, are specified using configuration wizard-like screens. The wizard-like screens also allow you to specify static network routes for sending information over the network, and to update or change the method by which the server keeps time.

Copying files 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 Release 5.2 implements upgrade improvements to provide a more robust system upgrade experience.

These upgrade improvements enable you to:

- Reduce 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.
- Support SCP and HTTPS protocols to allow secure file transfers.
- View 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, as shown in Figure 63, Figure 64, Figure 65, and Figure 66.

Figure 63: Method selection for file transfer

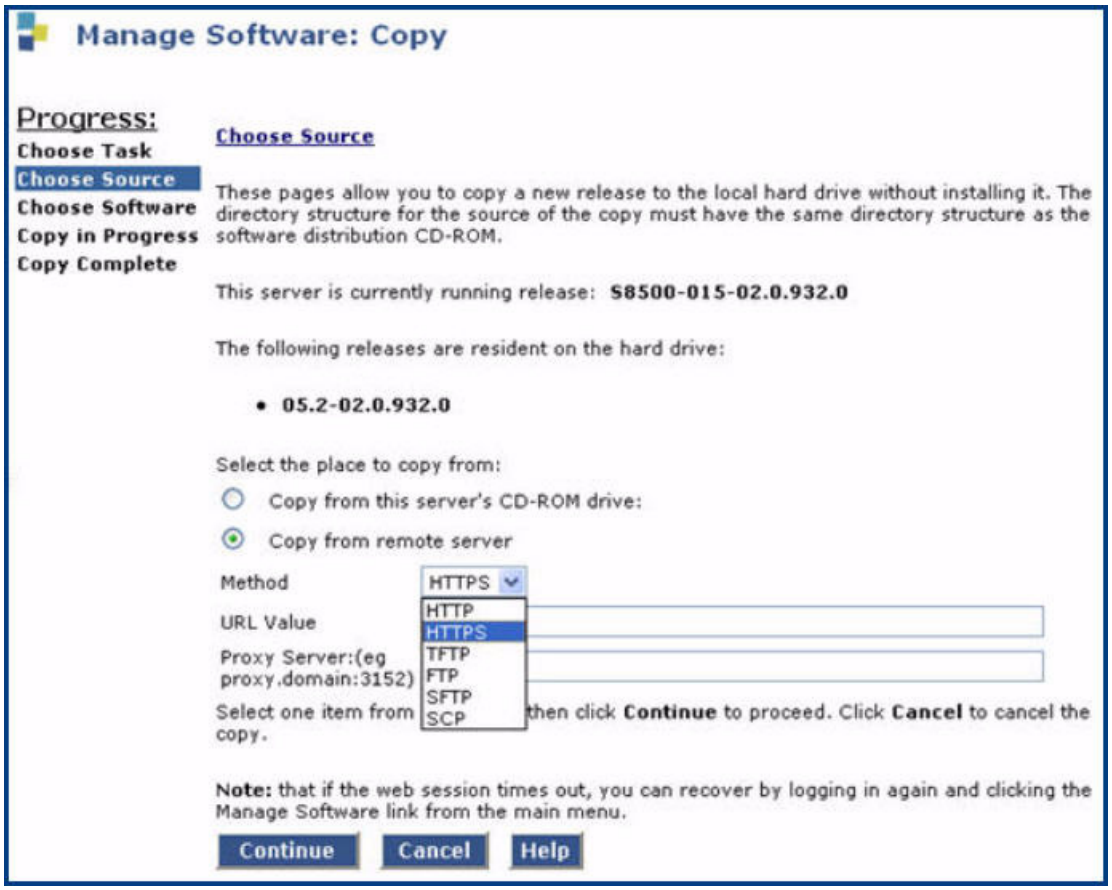


Figure 64: Detection of available release

Figure 65: Copy in progress

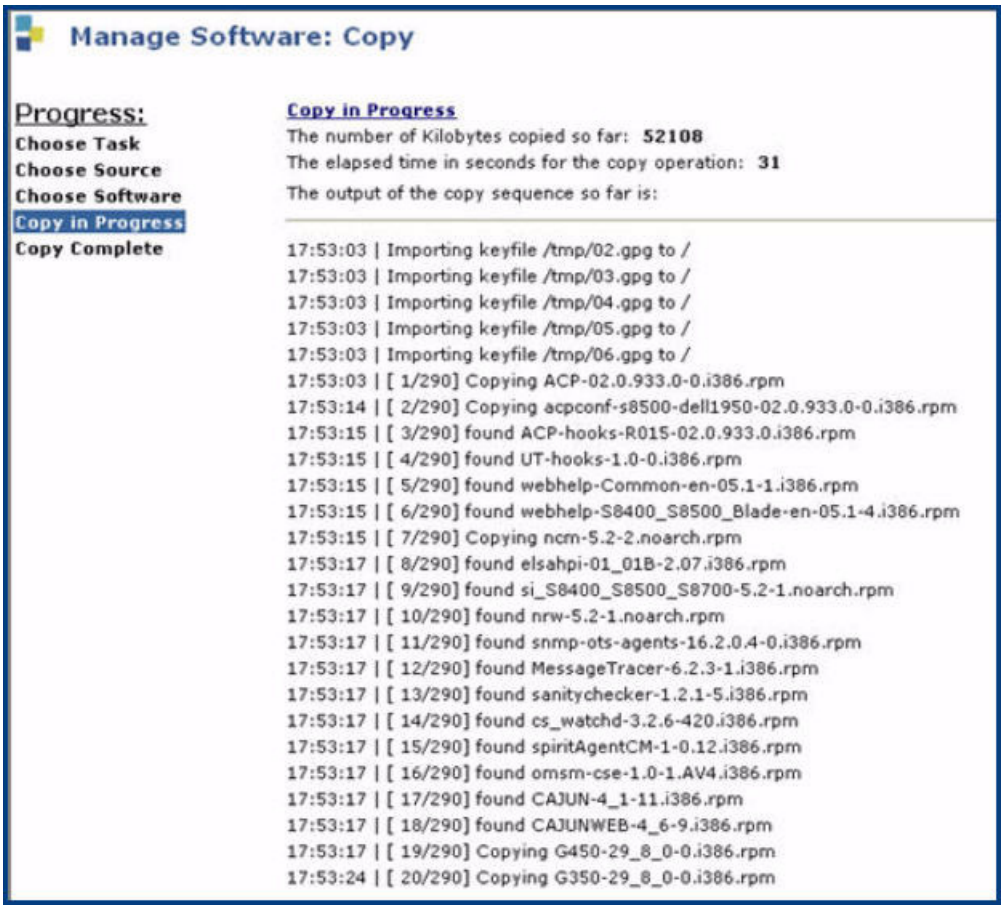
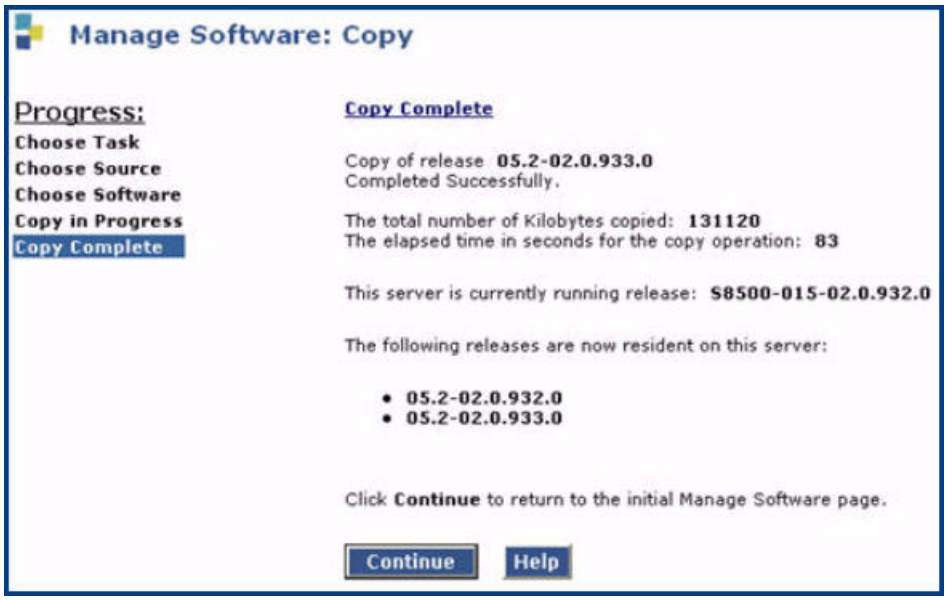


Figure 66: Copy complete



Setting up SNMP

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 Administering SNMP.

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 Using Device Manager to administer G700 Media Gateway components on page 497.

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.

Setting up Processor Ethernet

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 an LSP or an ESS server. Do not disable the PE interface on an LSP or an ESS server. Disabling the PE interface disables the LSP or ESS server's ability to register with the main server. The LSP or ESS 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 ESS 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.

Note:
PE on duplicated servers is supported only on S8720 and S8730 servers for endpoint, gateway, or adjunct connectivity in Communication Manager Release 5.2 and later. If you have an S8710 anywhere in your network, you cannot enable Processor Ethernet on any S87xx server without first upgrading the S8710 to an S8720 or S8730.

An LSP or a single ESS server can use the Processor Ethernet interface to connect to CDR, AESVCS, and CMS. Duplicated ESS servers can use the Processor Ethernet interface to connect to CDR, Messaging, and SIP Enablement Server (SES).

For more information on ESS, see *Using Avaya Enterprise Survivable Servers (ESS)*, 03-300428.

High-level steps to setting up the PE interface

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.

1. Load the Communication Manager software.
2. Load the license file.
3. 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 Set Identities page. The Set Identities page can be found on the server's System Management Interface select **Installation > Configure Server**.
   b. If this is an ESS server or an LSP, 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 LSP or ESS server will connect. The IP address is used by the LSP or ESS server to register with the main server. In a new installation, where the LSP or the ESS server has not received the initial translation download from the main server, this address will be the only address that the LSP or the ESS 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 LSP or the ESS server is also connected. The ESS server or the LSP 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.

4. On the Communication Manager System Access Terminal (SAT), enter the name for each ESS server, LSP, 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.
5. 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.
6. 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.
7. For adjunct connectivity to an ESS server or an LSP, 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 ESS server or the LSP in the remaining fields.
   - Disable the processor channel on the ESS server or the LSP by entering **n(o)** in the **Enable** field.
8. 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 ESS or LSP server.

Defining network port usage

The main server(s), LSPs, and each ESS server, use specific TCP/UDP ports across a customer's network for registration and translation distribution. Use the information in Table 9 to determine which TCP/UDP ports must be open in your network for an LSP or an ESS server. You must check the firewalls on your network to open the required TCP/UDP ports.

Table 9: 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	
		1 of 2

Table 9: Network port usage (continued)

Port	Used by:	Description
21873 (TCP port)	The main server(s) running Communication Manager 2.0 to download translations to the LSP(s).	Prior to an upgrade to Communication Manager 3.0 or later, servers running Communication Manager 2.x used port 21873 to download translations to the LSP(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 ESS server(s) and the LSP(s) on Communication Manager 3.0 and later loads.
		2 of 2

To configure the ports on your server, click **Firewall** under the **Security** heading in the Server Administration Interface (Figure 67).

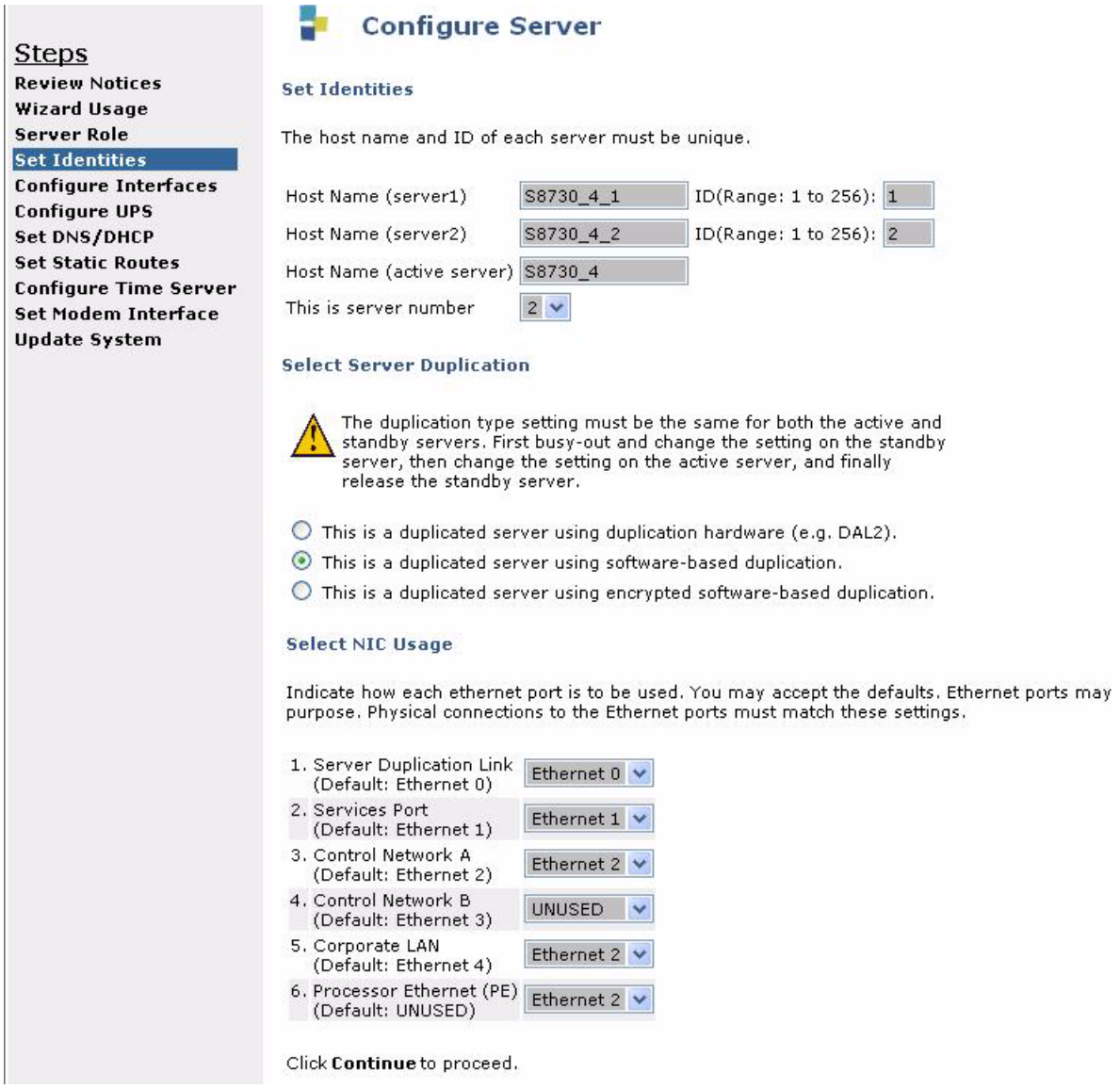
Figure 67: Firewall screen in the Server Administration Interface

Configuring the PE Interface

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.

Setting identities

Figure 68: Configure server - set identities page



This page is used to:

- Assign host name(s) and server ID(s) to this server
- Server Numbers (duplicated servers only)
- Select a duplication configuration (duplicated servers only) and
- Determine how Ethernet interfaces on this server will be used.

When this server is first installed, this page shows default values as appropriate for this particular server. Thereafter, this page shows configured values. The fields are as follows: Not all fields are used on all server models.

Host name: A host name is the name given to this server and is part of a Fully Qualified Domain Name or FQDN. For example, www.myserver.avaya.com is an FQDN and myserver is the host name. The host name can be any name you choose but must be unique in your network and should only contain letters, numbers and the under-bar (_) character.

ID: Each server within the enterprise is assigned a unique server ID (SVID). Gaps in the SVIDs are allowed. Each server in the system, duplicated or single, main server or ESS server, requires a unique SVID.

Server Number: This field appears only for duplicated servers. When servers are duplicated, one server is assigned server number 1 and the other number 2. The server assigned number 1 will be is preferred in server interchange decisions when the state of health of the two servers is equal.

Server Duplication: If this server is duplicated, the ability to select the type of duplication technology is provided. If a hardware duplication board is present, the ability to select hardware duplication is provided. If this board is not present, then only software duplication is shown and the only choice is to select encryption of the duplication link or not.

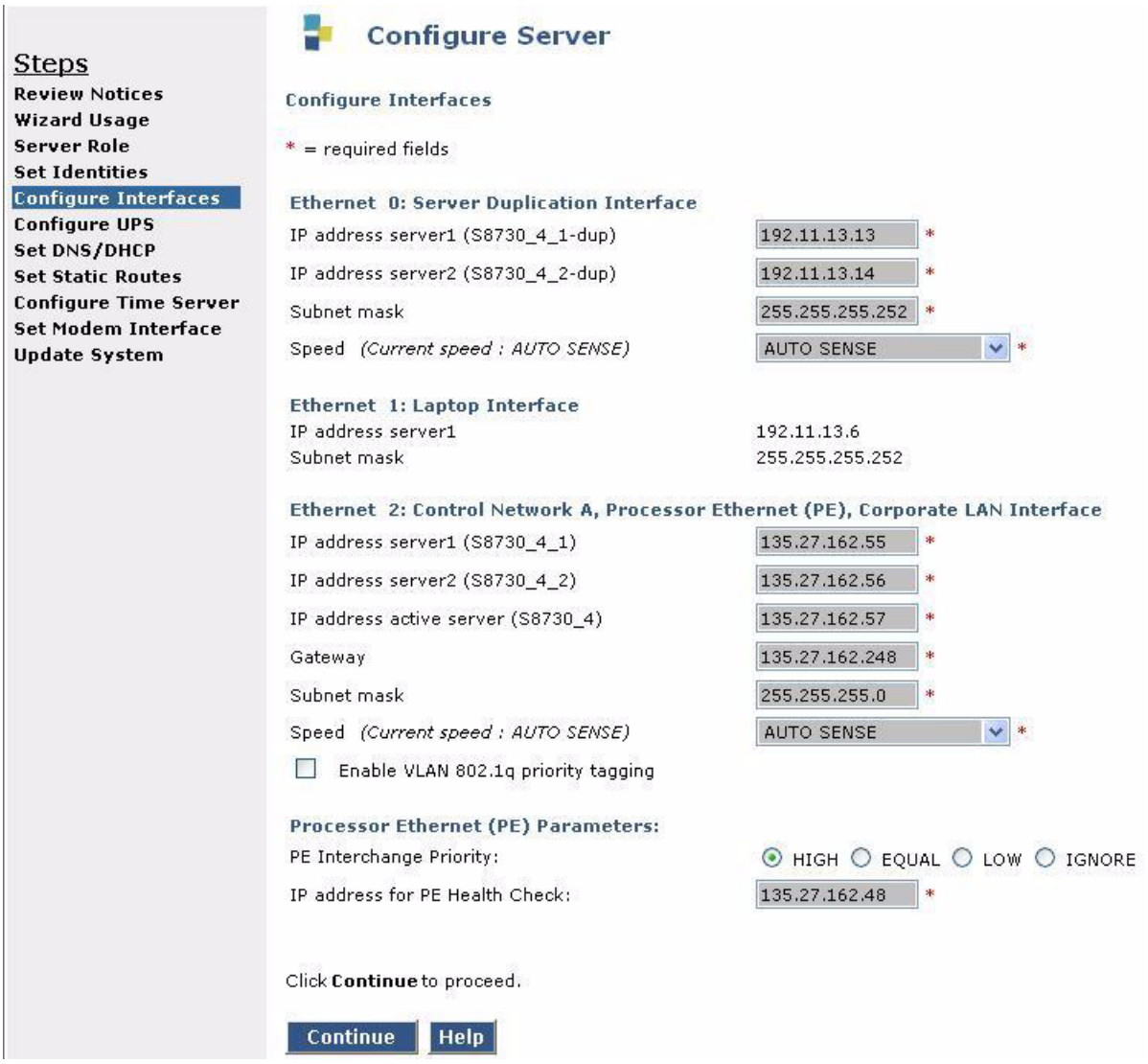
Note: Selecting encryption reduces the capacity of the server by approximately 25%.

Select NIC Usage: This section lists the functions that are supported on this server and allows those functions to be associated with a particular network interface. The possible functions are:

- Laptop Interface: The laptop function must be assigned to a NIC by itself. The laptop interface is not restricted by firewall rules and is designed for local connection of a services laptop.
- Duplication Link: The duplication link is the link that is used to shadow memory contents from the active server to the standby server in a duplicated pair. This link must be assigned to a gigabit Ethernet interface and must be assigned to a NIC by itself.
- Control Network A and Control Network B: These are the links that are used to communicate with the IP Serial Interfaces (IPSI) in a G650 gateway. If there is only one IPSI in each G650, then only control network A is assigned. If there are two IPSIs in each G650, then both control network A and control network B are assigned.
- Enterprise LAN: The enterprise LAN is the primary interface for system administration.
- Processor Ethernet: The Processor Ethernet or PE interface is a special interface that is used like or in place of a C-LAN interface. IP telephones, trunks and certain adjuncts may connect to the PE interface. *The PE interface must be assigned to the same NIC as the enterprise LAN*.

Configure interfaces

Figure 69: Configure interfaces page



This page is used to configure IP addresses for the network interfaces that were assigned in the Set Identities page and to configure special parameters for the Processor Ethernet (PE) interface on duplicated servers. A red asterisk (*) marks a field that is a required entry.

When entering values in this page the following must be noted:

1. The NIC used for the laptop interface is automatically assigned fixed values that cannot be changed.

2. When entering information for duplicated servers, enter IP addresses consistent with how these servers were assigned server numbers on the Set Identities page.
3. The address assigned to the active server on duplicated servers is what the industry knows as an IP-alias. The active server in a duplicated pair of Communication Manager servers will respond on this address; the standby server in the pair will not. If a server interchange occurs, the server that becomes the active server will re-associate its MAC address with the active server IP address. It is very important to assign the *same* IP address to the active server entry on both servers in a duplicated pair of servers. The NIC being assigned an active server address will have two IP addresses associated with it, a server unique address assigned as IP address server1 or IP address server2 and an alias address assigned as the IP address active server. A pair of duplicated servers will then require three IP addresses, one unique to each server and a third for the alias. All three addresses must be on the same subnet.
4. The terms IP address, (default) gateway, subnet mask, speed, and VLAN tagging are used in the standard industry manner.
5. Verify with the network administrator that the LAN hardware supports 802.1q priority tagging. If supported, select **VLAN 802.1q priority tagging**.

Processor Ethernet (PE) Parameters

Two special parameters appear when Processor Ethernet is assigned on a duplicated pair of servers. These parameters control how the health of the PE interface affects server interchange decisions and how the system determines whether the PE interface is working or not (PE state of health).

PE Interchange Priority

Assign the PE a simple relative priority as compared to IPSIs in configurations that use both PE and IPSIs. The priority levels are as follows:

- **PE = HIGH** Favor the server with the best PE SOH when PE SOH is different between servers.
- **PE = LOW** Favor the server with the best IPSI connectivity when IPSI SOH is different between servers.
- **PE = EQUAL** Count the PE interface as one IPSI and favor the server with the best connectivity count.
- **PE = IGNORE** Do not consider the PE in server interchange decisions.

IP Address for PE Health Check

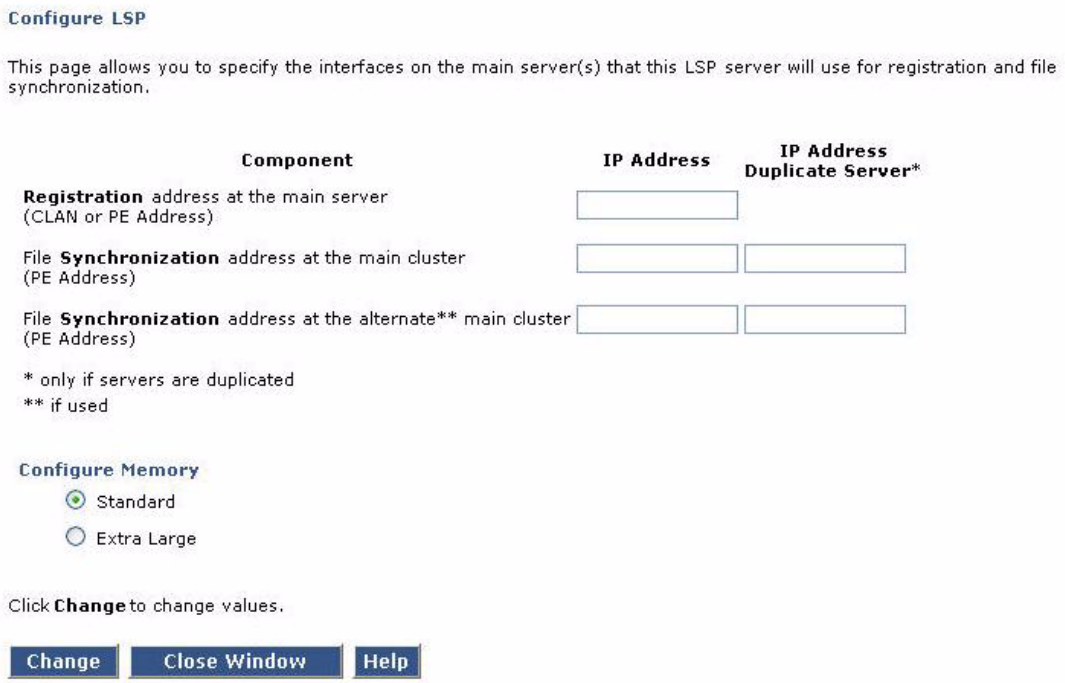
Enter the IP address to enable the server to determine whether its PE interface is working or not. The network gateway router is the default address. Any device on the network that will respond can also be used.

Configuring an LSP or an ESS server

When configuring an ESS server or an LSP you must complete the Configure Server - Configure LSP or ESS screen in addition to the Set Identities screen. Figure 70 and Figure 71 show an example of the Configure LSP or ESS screen.

Figure 70: Configure server - specify a server role

Figure 71: Configure server - configure an LSP or an ESS server



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

1. Select the radio button next to the correct entry to indicate if this is an ESS server, an LSP, or neither an ESS server or an LSP.
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 LSP or ESS server is also connected. The IP address is used by the LSP or ESS server to register with the main server. In a new installation, where the LSP or the ESS server has not received the initial translation download from the main server, this address will be the only address that the LSP or the ESS 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 LSP or the ESS server is also connected. The ESS server or the LSP 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

Use the command **`set mgc list`** on an H.248 gateway when adding a PE-enabled S8500 or S8300 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>`***

Administering PE in Communication Manager

Processor Ethernet administration is always performed on the main server. The LSP or the ESS 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 LSP or an active ESS server. In this case, the administration is temporary until the communication to the main server is restored. At that time, the LSP or the ESS 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 S8300, S8400, or an S8500 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 ESS server or the LSP is using the PE interface. The IP Interfaces screen is automatically populated for an ESS or LSP.

- Survivable Processor screen

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

Administering ESS servers for PE

If there is an ESS server in the configuration, you must add the ESS server using the Survivable Processor screen. For more information on administering the ESS server on the Survivable Processor screen, see *Using Avaya Enterprise Survivable Servers (ESS)*, 03-300428.

Administering LSP servers for PE

Local Survivable Processors (LSPs) are administered using the Survivable Processor screen. For more information on administering an LSP, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Working with adjuncts

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 LSP and the ESS server, there are three adjuncts, the CMS, AESVCS, and the CDR, that are supported using the LSP or the ESS server's PE interface. This section provides a high-level overview of the adjuncts supported by the ESS server and the LSP 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 ESS server or LSP. A Survivable CMS is a standby CMS that collects data from an LSP or an ESS 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 ESS server or the LSP, but does not collect data or support report users. Only the main CMS server collects data. When an ESS server assumes control of one or more port networks, or an LSP is active, the ESS server and/or the LSP 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 an ESS server or LSP, 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 an LSP or an ESS server, you must administer the Survivable Processor screen in addition to the IP Services screen.

Using load balancing

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 **1** 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.

Setting 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 Using load balancing on page 522.

Administering the main or LSP split registration

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

The split registration 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 LSP.

Detailed description

Avaya provides the following alternatives for managing split registrations:

- 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 LSPs or between an ESS and LSPs. This solution does not handle split registration between a main server and an ESS.

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

When aggregation at the LSP is preferred, the main server or ESS disables the network regions associated with the LSP, forcing all the telephones and gateways in the regions to register with the LSP. Re-registration to the main server or ESS 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 LSP is backing up.
- The **`enable mg-return`** command is executed. After re-registration to the main server or ESS starts, it continues until the LSP reports inactive status, one hour elapses since execution of the **`enable mg-return`** command, or until you run the **`disable mg-return`** command.
- The LSP unregisters from the main server or ESS.

Split registration 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 LSP or the main server. When administered or set, telephones and gateways can be forced to register with active LSPs. The split registration solution keeps branch-oriented operations intact with local trunk resources.

LSPs 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 LSPs.

Sequence of events

The administrator enables the split registration 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 an LSP.
2. The LSP 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 LSP.
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.

Considerations

Network design notes for split registration solution

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

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

  The execution of **`enable nr-registration`** [**`enable network region registration`**] in a region puts a region to auto disable (**ad**) if the LSP backing the region is active. All other regions backed up by that LSP 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 feature.
- An ESS allows LSPs 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 an LSP, the LSP 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 an ESS.
- Split registrations between the main server and ESS may occur if the ESS'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 ESS in AGLs. If a Telephone registers to a C-LAN controlled by an ESS, 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 LSP 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 an LSP entry under the column heading BACKUP SERVERS IN PRIORITY ORDER to be changed if the corresponding LSP 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 LSP's address at the end of the list. If the LSP'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 LSP.

Network region type description

An LSP is administered as a backup server for one or more network regions. The LSP can have resources from one or more network regions. When the LSP 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.

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

Implementation procedures

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

Prerequisites and constraints

The main server, LSP and ESS must be running on Communication Manager 5.2.

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

To administer the split registration 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 LSP entry. The number of non-LSP entries in this column is not affected. After implementing the split registration solution, only one LSP entry is allowed under BACKUP SERVERS IN PRIORITY ORDER.

Administration procedures

The administrator performs the following procedures to enable and disable the split registration solution:

Enforcing the split registration solution

1. Type **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. Press **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 LSP is listed as a Backup Server for each ip-network-region.

Disabling the split registration solution

1. Type **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. Press **Enter** to save your changes.

Note:
You can set **Force Phones and gateways to Active LSPs** to **n** only if all registered LSPs 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 LSP also return to the main server.

Gateways and Endpoints can return to the main server if the LSP unregisters from the main Communication Manager server.

Return to main server continues till at least one of the following events occur:

- The LSP 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 Enterprise Survivable Servers (ESS) or Local Survivable Processor (LSP).

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 LSPs 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 LSPs 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 Administration procedures.

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 available C-LAN from within the 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 are 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 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 **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) and establish a socket to Communication Manager after Registration Admission Status (RAS) is completed.

Socket load balancing for TTS telephones occur after registration is complete and the AGL is formed. Communication Manager initiates socket establishment to TTS telephones. 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 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, and indirect) and sends a subset of the C-LANs starting at a random place in the C-LAN array.

Building the Alternate Gatekeeper Lists

Communication Manager 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 using the 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 enhancement of this feature is that the 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 builds the Alternate Gatekeeper Lists.

Application

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

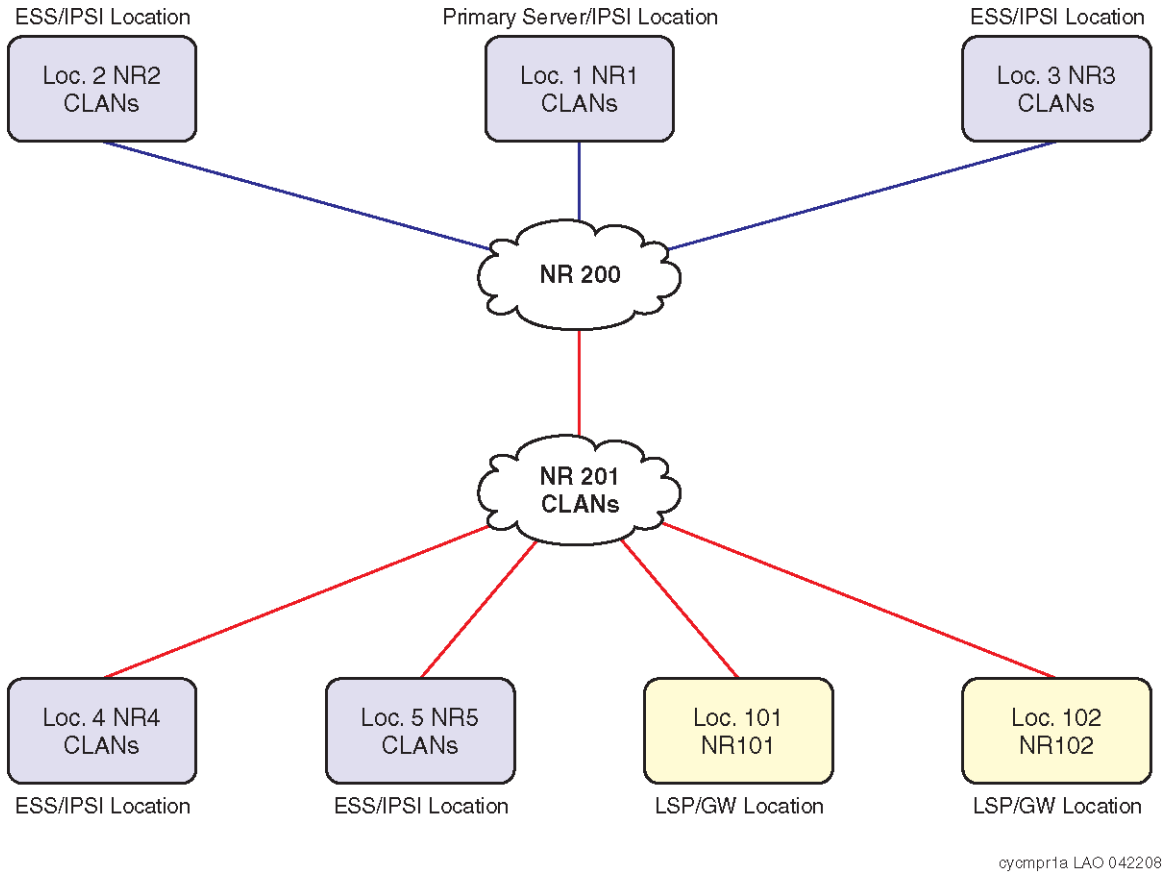
The examples are based on configurations using WAN facilities.
In both examples, a virtual network region is assigned to the WAN to describe the WAN topology, and to implement Call Admission Control (CAC).

- 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.

Example 1: Unwanted C-LANs in the AGL

Figure 72 shows how unwanted C-LANs can end up in the Alternate Gatekeeper List.

Figure 72: Unwanted C-LANs in 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.

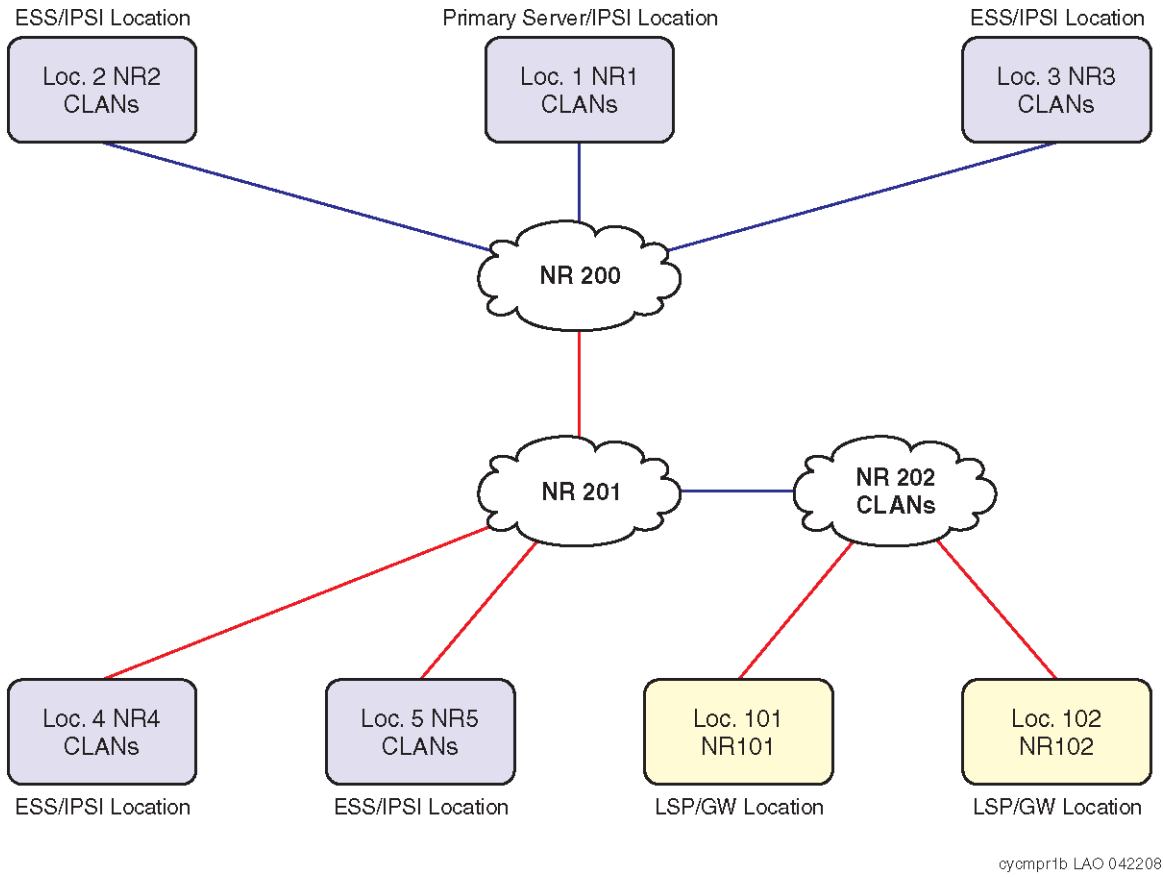
NR4 and NR5 are ESS locations, and the IP telephones in those two locations need local C-LANs that are in NR4 and NR5.

NR101 and NR102 are Gateway/LSP locations and should share pooled C-LANS. In this case, C-LANS are placed in NR201 as they are directly connected to the two NRs. In Communication Manager Release 5.1 and earlier, 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 an ESS.

Figure 73 shows the workaround that you can implement using another virtual network region in earlier releases of Communication Manager.

Figure 73: Earlier releases of CM 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 ESS. This workaround does not address the size of the AGL.

Figure 74 shows the improved configuration of the network region using the Administrable AGL feature for Communication Manager.

Figure 74: Improved configuration for unwanted C-LANs using enhanced AGL feature

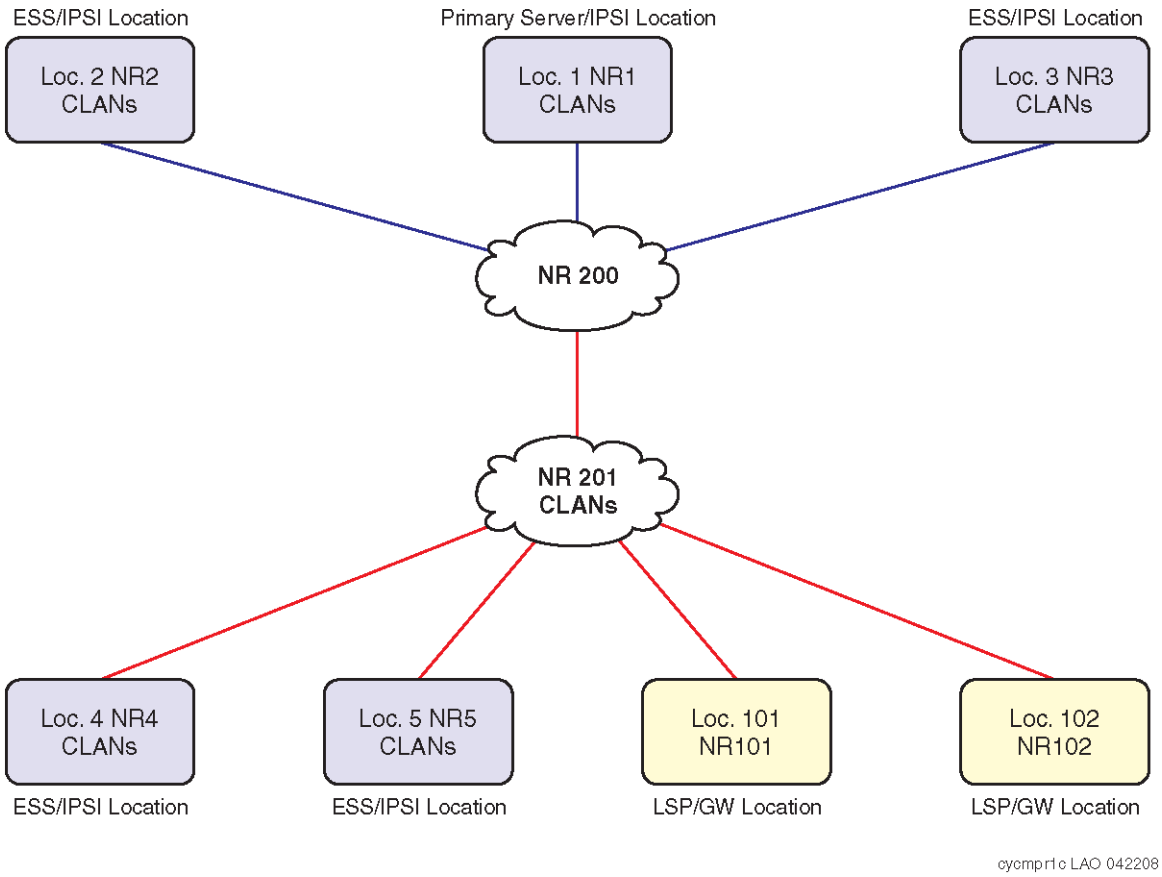


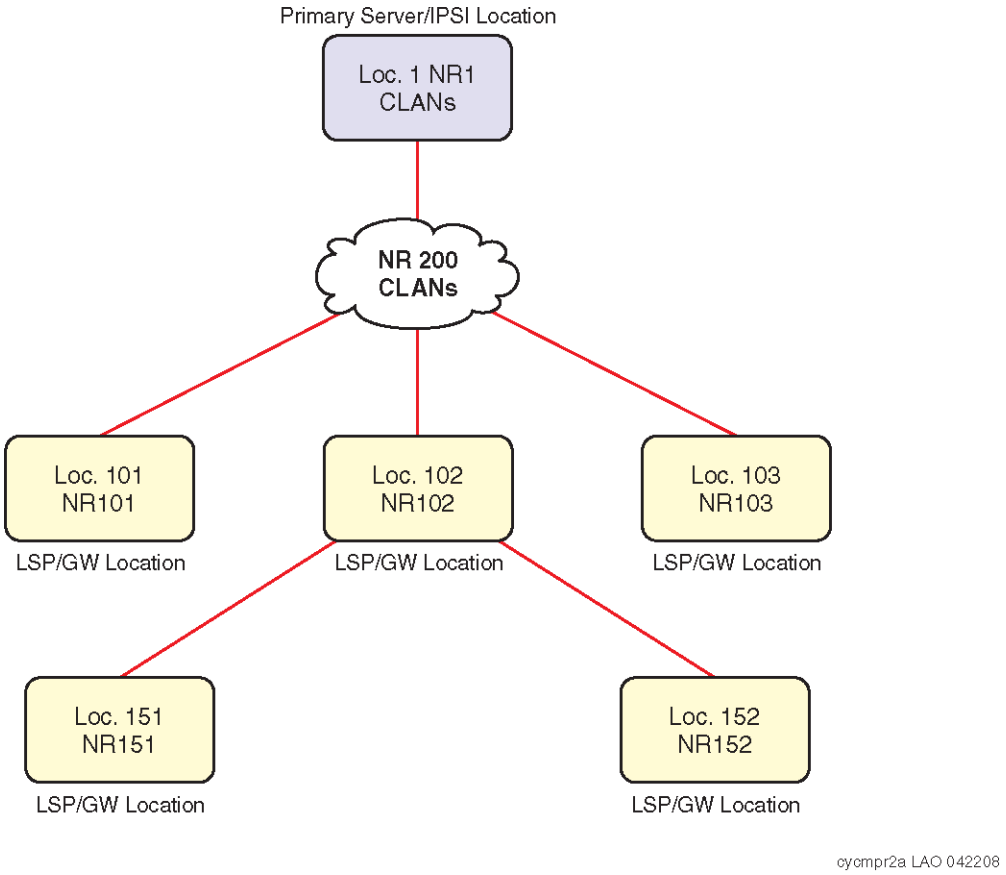
Figure 74 shows a configuration in which the IP telephones in NR4 and NR5 are administered to only use C-LANS in their native NR, and not use C-LANs in NR201. The IP telephones AGLs in NR4 and NR5 contain local C-LANs. The IP telephones in NR101 and NR102 share C-LANs in NR201. Those C-LANS are physically 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 ESS.

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

Example 2: Unable to pool C-LANS because of Network Region Connectivity

Figure 75 shows how network region connectivity issues can prevent the pooling of C-LANs.

Figure 75: Inadequate pooling of C-LANs

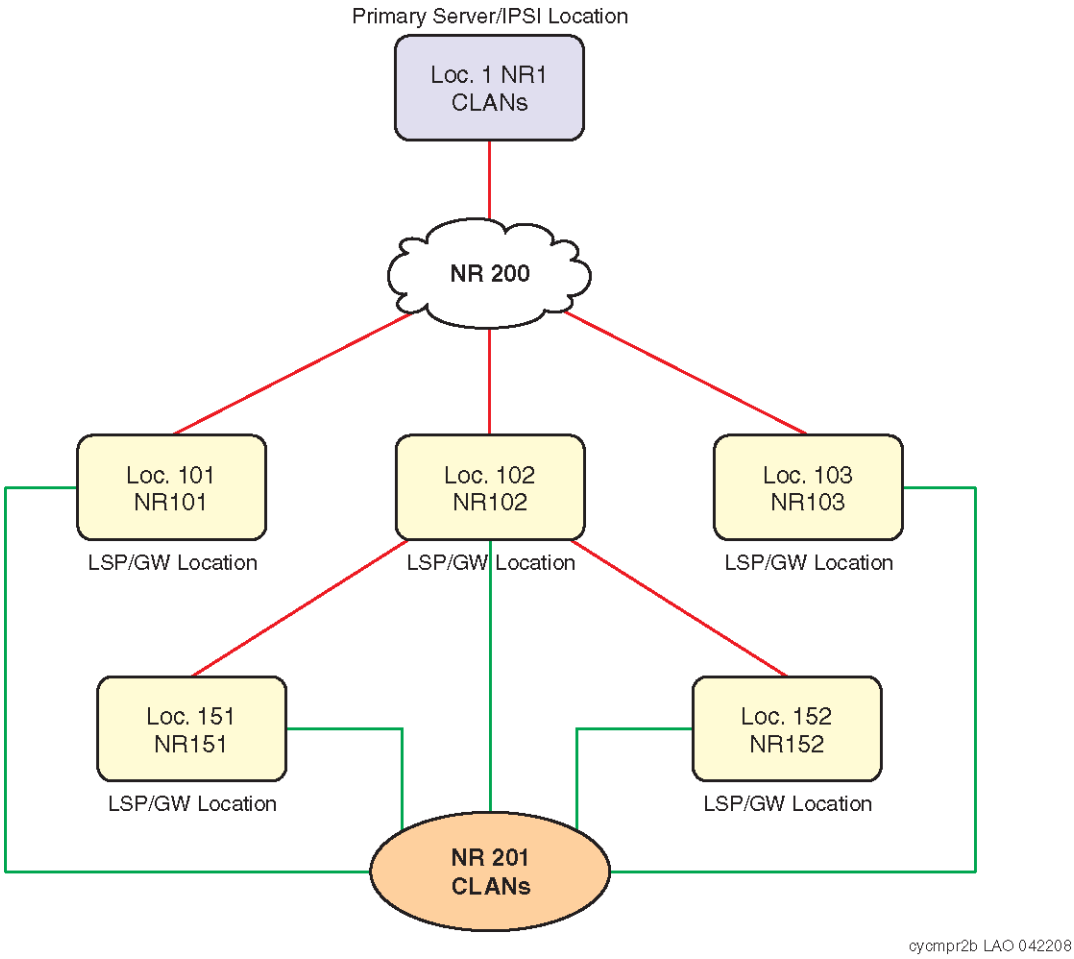


The figure shows a network configuration with numerous Gateway/LSP locations, some of which are directly connected to the WAN, and others that are indirectly connected to the WAN. All of these gateways need to share a pool of C-LANS physically located at location 1.

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 the size of the AGL.

Figure 76 shows the workaround that you can use with earlier releases of Communication Manager software.

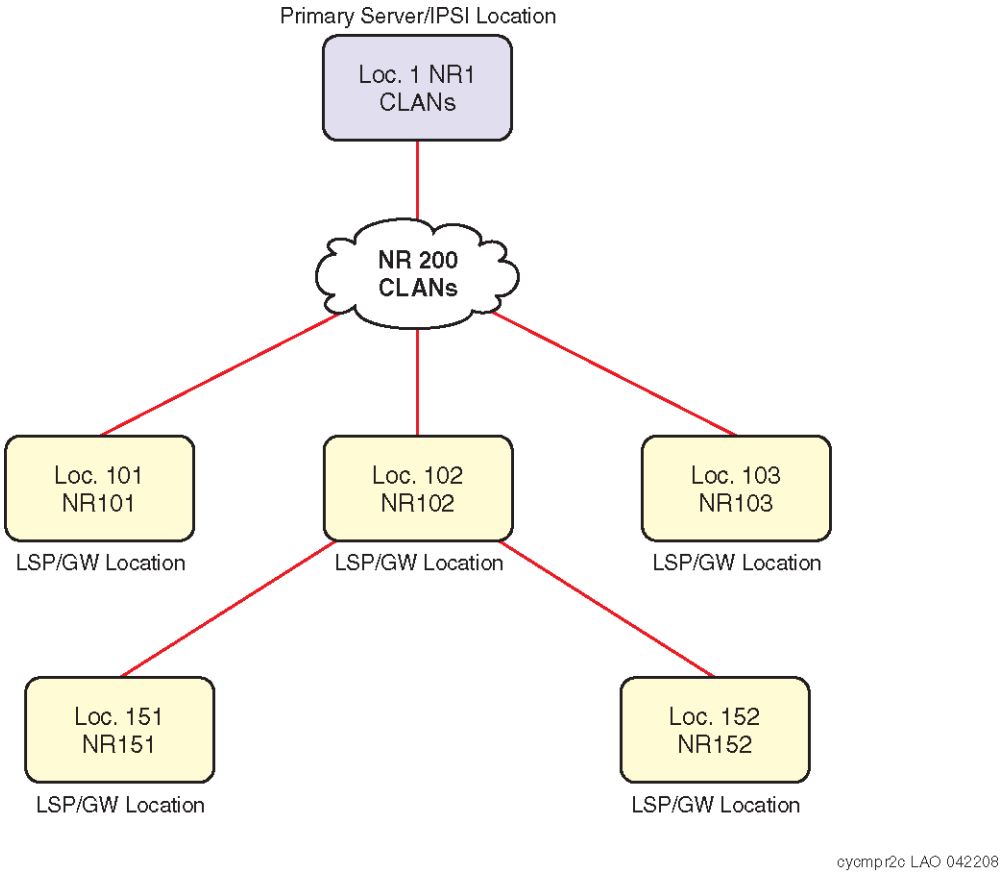
Figure 76: Earlier releases of CM workaround for inadequate pooling of C-LANs



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 the number of C-LANs in NR201 that you can use to control size of AGL. This configuration does not reflect the WAN topology.

Figure 77 shows the improved configuration using the Communication Manager Administrable AGL feature.

Figure 77: Improved configuration using the CM 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.

High-level capacities

The total AGL assignments for each source region must add up to 16 or lower. Each source network region can continue to have 6 LSPs 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, LSP for each region and the Survivable Gatekeeper for the station).

Considerations

If the telephone's IP address is in one of the ranges in the ip-network-map, the AGL entries consist of the C-LANs or PE from the telephone's home region, directly connected regions, and indirectly connected regions. If the IP address is not in one of those ranges, the AGL entries consist only of the C-LANs or PE from the telephone's home region.

Interactions

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

- It is possible to have some regions using the earlier releases of Communication Manager 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 telephone registrations and H.323 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 SIP telephones register to SES.
- If an extension number has shared control using the server between a H.323 telephone and a H.323 softphone, Communication Manager shows on the Status Station screen both the AGL sent to the H.323 telephone and the H.323 softphone. See Verifying AGL settings for stations on page 540 for more information.
- In Communication Manager Release 5.1 or earlier, 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). In Communication Manager Release 5.2, 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 Administrable AGL feature, you should not use C-LAN priorities.

Note:
Remember the following additional information:

- For TTS telephones, the Communication Manager takes into consideration priorities, C-LAN socket load, and C-LAN's service state and whether the C-LANs are allowed to be used for H.323 telephone registration when load balancing.

- For non-TTS telephones, priorities and C-LAN socket load are taken into account when load balancing.
- For TTS and non-TTS telephones, the Communication Manager does *not* take either priorities or C-LAN socket load into consideration when building the AGL.

Prerequisites

- Communication Manager Release 5.1 or later
- Basic administration procedures for H.323 telephones

Administration procedures

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

Configuring Administrable Alternate Gatekeeper Lists

To configure the Administrable Alternate Gatekeeper Lists:

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. Press **Enter** to save your changes.

Viewing IP Network Maps for your system

To view the IP Network Maps for your system:

1. Enter **`change ip-network-map`**.

   The system displays the IP Address Mapping screen.
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 and press **Enter** to save your changes and exit the screen.

Verifying AGL settings for stations

To verify the AGL settings for stations:

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. The system displays the Status Station screen.
2. Page down till you find the page for the Alternate Gatekeeper List.

Figure 78: IP Address Mapping screen

```
status station 51113                              Page   7 of   x
                            ALTERNATE GATEKEEPER LIST
          Main             Shared Control Ports      Shared Control Ports
Node Name        Region   Node Name        Region   Node Name        Region
sraychk-clan2      3




For the LSP entries: BACKUP SERVERS on ip-network-region [Set-end Rgn number].
For the Survivable Gatekeeper entry: display station [extension].
```

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 and press Enter to exit the screen.

IP Network Region Connection Management screen

- The AGL field in the IP Network Region Connection Management screen. Values are between **0** through **16**; or the field is **all** or blank. See Configuring Administrable Alternate Gatekeeper Lists for more information on the values.

Figure 79: Alternate Gatekeeper List on Status Station

```
status station 51113                              Page   7of   x
                            ALTERNATE GATEKEEPER LIST
          Main             Shared Control Ports      Shared Control Ports
Node Name        Region   Node Name        Region   Node Name        Region
sraychk-clan2      3




For the LSP entries: BACKUP SERVERS on ip-network-region [Set-end Rgn number].
For the Survivable Gatekeeper entry: display station [extension].
```

Field descriptions

Table 10: Field descriptions

Field	Description
Main	Refers to the IP telephone.
Shared control	See section titled Control of DCP Telephone in the *Avaya Aura™ Communication Manager Screen Reference*, 03-602878
Node name	Identifies the name of the adjunct or server/switch node. See the IP Node Name screen in the Screen Reference section of the *Avaya Aura™ Communication Manager Screen Reference*, 03-602878
Region	The number of the region. See the description for the IP Network Region screen in the Screen Reference section of the *Avaya Aura™ Communication Manager Screen Reference*, 03-602878

Troubleshooting scenarios and repair actions

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

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
- *Using Avaya Enterprise Survivable Server (ESS)*, 03-300428
- *Application Notes for Administrable Alternate Gatekeeper List for IP Phones Using Avaya Communication Manager*, Issue 1.0
- *Avaya 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 ESS **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.

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.

Survivability

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

Administering Call-processing

The telephony features of the S8300 Server are administered using the same commands and procedures as an S8700-Series Server or a legacy DEFINITY Enterprise Communications System.

Accessing Communication Manager

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.

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. ASA is available in several languages.

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 Chapter 1: 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 G700 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 Backing up and restoring data on page 502).
- Support for RADIUS authentication for media gateways and P330 stack elements using the P330 Device Manager. See Using Device Manager to administer G700 Media Gateway components on page 497.

Command syntax changes for media modules

The syntax for using the SAT commands for a G700 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.

Accessing the Communication Manager SAT CLI

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

- Using Secure Shell for remote login on page 546
- Using Telnet over the Customer LAN on page 548
- Using Avaya Terminal Emulator for LAN connection to Communication Manager on page 553
- Using Windows for PPP modem connection (Windows 2000 or XP) on page 550

  This connection requires you to have a modem on your PC. It also requires you to do the following first:

  - Setting up Windows for Modem Connection to the Avaya S8xxx Server (Windows 2000 or XP) on page 548
  - Configuring the remote PC for PPP modem connection (Windows 2000 or XP, Terminal Emulator, or ASA) on page 549
- Using Avaya Terminal Emulator for Modem Connection to Communication Manager on page 554

  This connection requires you to have a modem on your PC. It also requires you to do the following first:

  - Setting up Windows for Modem Connection to the Avaya S8xxx Server (Windows 2000 or XP) on page 548
  - Configuring the remote PC for PPP modem connection (Windows 2000 or XP, Terminal Emulator, or ASA) on page 549
- Configuring Avaya Site Administration on page 21

Using Secure Shell for remote login

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

- G350 Media Gateway
- S8300, S8400, S8500, or S8700-Series Server 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. For details on disabling Telnet, see Turning off Telnet for increased security on page 548.

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

Prerequisites:

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

To enable a secure FTP (SFTP) session on a C-LAN or VAL circuit pack:

1. Type **`enable filexfr [board location]`**. Press **Enter**.

   The system displays the **Enable File Transfer** screen.
2. Type a 3-6 alphabetic character login in the **Login** field.
3. Type a 7-11 character password (one character must be a number) in the first **Password** field.
4. Retype the same password in the second **Password** field.
5. Type **y** in the **Secure?** field. Press **Enter**.

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

To disable a secure FTP (SFTP) session on a C-LAN or VAL circuit pack:

1. Type **`disable filexfr [board location]`**. Press **Enter**.

   SFTP is disabled on the circuit pack.

Using Telnet over the Customer LAN

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.

To use Telnet over the customer LAN:

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**.
   - Type **`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, type 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.

   The system displays the SAT command line.

Turning off Telnet for increased security

If you are using SSH to log in to the server or gateway, you might wish to turn off Telnet for an extra level of security. To turn off Telnet:

1. On the Server Administration Interface main menu, under **Security**, click on **Firewall**.

   The system displays the Firewall page.
2. Click the **Telnet Input to Server** boxes so that the check mark disappears.
3. Click the **Telnet Output from Server** box so that the check mark disappears.
4. Click the **Submit** button.

Setting up Windows for Modem Connection to the Avaya S8xxx Server (Windows 2000 or XP)

Note:
The remote dial-up PC must be configured for PPP access. Also, Avaya Terminal Emulator does *not* support Windows XP.

To set up Windows for Modem Connection:

1. Right-click **My Network Places** and click **Properties**.
2. Click **Make New Connection** and follow the Network Connection Wizard:
3. Select **Dial-up to private network** on the Network Connection Type screen.
4. In the **Phone number** field, enter the appropriate telephone number inserting special digits such as 9 and 1 or *70, if necessary.
5. On the Connection Availability screen, click **For all users** or **Only for myself**, as appropriate.
6. On the Completing the Network Connection Wizard screen, type the name you want to use for this connection. This name will appear in the **Network and Dial-up Connections** list.
7. Check **Add a shortcut to my desktop**, if desired, and click **Finish**.
8. If a Connect screen appears, click **Cancel**.

Configuring the remote PC for PPP modem connection (Windows 2000 or XP, Terminal Emulator, or ASA)

To configure the remote PC for PPP modem connection:

1. On your PC's desktop, right-click **My Network Places** and click **Properties**.

   The system displays the Network and Dial-up Connections screen.
2. Double-click the connection name you made in the previous task, Setting up Windows for Modem Connection to the Avaya S8xxx Server (Windows 2000 or XP) on page 548.

   Note:
   Depending on your system, the Connect screen might appear, from which you must select **Properties**.
3. Click the **Security** tab.
4. Select the **Advanced (custom settings)** radio button.
5. Check the **Show terminal window** check box.
6. Click the **Networking** tab.
7. In the **Components** box, verify that **Internet Protocol (TCP/IP)** and **Client for Microsoft Networks** are both checked.
8. Select **Internet Protocol (TCP/IP)** and click **Properties**.
9. Click the **Advanced** button.
10. Clear the **Use default gateway on remote network** box.
11. Click **OK** three times to exit and save the changes.

Using Windows for PPP modem connection (Windows 2000 or XP)

This connection requires you to have a modem on your PC. It also requires you to do the following first:

- Setting up Windows for Modem Connection to the Avaya S8xxx Server (Windows 2000 or XP) on page 548
- Configuring the remote PC for PPP modem connection (Windows 2000 or XP, Terminal Emulator, or ASA) on page 549.

To use Windows for PPP modem connection:

1. Return to the Network and Dial-up Connections screen and right-click the connection you just created.
2. Select **Connect**.
3. Leave the **User Name**, **Password**, and **Domain** fields blank. If the **Dial** field is blank, enter the appropriate telephone number.
4. Click the **Dial** button. When the Avaya S8xxx Server's modem answers, the system displays the After Dial Terminal screen.
5. Log on to the LAN.
   a. Enter your remote access login name and password.
   b. When the **Start PPP Now!** message appears, click **Done**.
   c. The system displays a small double-computer icon in the lower right portion of your screen.
6. Double-click the double-computer icon.
7. The system displays the connection's **Dialup Status** box.
8. Click on the **Details** tab.
9. Note the **Server** IP address.
10. Open a telnet session to the Avaya S8xxx Server:

    Type **`telnet <ip-address>`**, where ***`<ip-address>`*** is the Server IP address as noted in the **Dialup Status** box from Step 9.
11. Access SAT or use the CLI commands as needed.

International modem settings

You can change modem settings for a specific country using the Linux command line. To enter AT commands from a Linux command prompt:

1. On the command line, type (without quotes): **cu -l /dev/ttys1**, where -l is a lowercase L. Replace "ttyS1" with the tty port for the USB (e.g., /dev/usb/ttyACM0 for USB port 1). Press **Enter**.

   The system displays a "Connected" message.

2. Type **`ATI`**. Press **Enter**.

   The system displays an **OK** message.

3. Type the appropriate AT command to change the modem setting for the desired country. For example, for Japan, type **AT%T19,0,10&W0**. Press **Enter**.

   The system displays an **OK** message.

4. To return to the command prompt, type "**~**" (without quotes).

The following table shows AT commands and result codes for country-specific modem configuration

:

Country	AT Command (Hexadecimal)	Result Code (Decimal)
Argentina	AT%T19,0,34	52
Australia	AT%T19,0,01	1
Austria	AT%T19,0,34	52
Belgium	AT%T19,0,34	52
Brazil	AT%T19,0,34	52
Canada	AT%T19,0,34	52
China	AT%T19,0,34	52
Cyprus	AT%T19,0,34	52
Czech Republic	AT%T19,0,25	37
Denmark	AT%T19,0,34	52
Finland	AT%T19,0,34	52
France	AT%T19,0,34	52
Germany	AT%T19,0,34	52
		1 of 3

Country	AT Command (Hexadecimal)	Result Code (Decimal)
Greece	AT%T19,0,34	52
Hong Kong	AT%T19,0,30	48
Hungary	AT%T19,0,30	48
Iceland	AT%T19,0,34	52
India	AT%T19,0,30	48
Indonesia	AT%T19,0,30	48
Ireland	AT%T19,0,34	52
Italy	AT%T19,0,34	52
Japan	AT%T19,0,10	16
Korea	AT%T19,0,30	48
Liechtenstein	AT%T19,0,34	52
Luxembourg	AT%T19,0,34	52
Mexico	AT%T19,0,34	52
Netherlands	AT%T19,0,34	52
New Zealand	AT%T19,0,09	9
Norway	AT%T19,0,34	52
Philippines	AT%T19,0,30	48
Poland	AT%T19,0,30	48
Portugal	AT%T19,0,34	52
Russia	AT%T19,0,34	52
Singapore	AT%T19,0,30	48
South Africa	AT%T19,0,35	53
Slovak Republic	AT%T19,0,34	52
Slovenia	AT%T19,0,30	48
Spain	AT%T19,0,34	52
Sweden	AT%T19,0,34	52
		2 of 3

Country	AT Command (Hexadecimal)	Result Code (Decimal)
Switzerland	AT%T19,0,34	52
Turkey	AT%T19,0,34	52
United Kingdom	AT%T19,0,34	52
United States	AT%T19,0,34	52
		3 of 3

Enabling transmission over IP networks for modem, TTY, and fax calls

Prerequisites

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.

To enable transmission over IP networks for modem, TTY, and fax calls:

1. Type **`change ip-codec-set 1`**. Press **Enter**.

   The system displays the IP Codec Set screen.

Complete the fields as required for each media type you want to enable. Press **Enter**.

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

Using Avaya Terminal Emulator for LAN connection to Communication Manager

You can download the Avaya Terminal Emulator from the main menu for the VisAbility Management Suite. Simply click **Download** next to the Administration menu item and follow the instructions.

Once the Terminal Emulator is installed on your PC, use the following steps to establish a LAN connection to your Avaya S8xxx Server.

1. Double-click the Terminal Emulator icon on your desktop. Alternatively, go to the Start menu, select Programs, then Avaya, then Terminal Emulator.

   The system displays the Terminal Emulator.
2. From the menu bar across the top of the screen, select **Phones**, then select **Connection List**.

   The system displays the Connections screen.
3. From the menu bar across the top, select **Connection**, then select **New Connection**.

   The system displays the Connection Settings screen.
4. Put in a name for the connection. Usually, this will be the name of your Avaya S8xxx Server.
5. On the Host screen, click **Telnet**.
6. Click the **Emulation** tab at the top.

   The system displays the **Emulation** tab.
7. From the Emulator drop-down box, select the emulator you desire, usually **513BCT** (default), **AT&T 4410, AT&T**, or **DECVT100**.
8. In the Keyboard window, select **pbx**.
9. Click the **Network** tab.

   The system displays the **Network** tab.
10. In the **IP address** field, type the IP address of the Avaya S8xxx Server.
11. In the **TCP/IP port number** field, type **5023** to log in directly to the Communication Manager SAT command line.
12. Click **OK**.

    The Connection Settings screen disappears.
13. On the Connections screen, double-click the name of the connection you just set up.

    The Login prompt for the Communication Manager software appears.
14. Log in to Communication Manager to access the SAT command screen.

Using Avaya Terminal Emulator for Modem Connection to Communication Manager

This connection requires you to have a modem on your PC. It also requires you to do the following first:

- Setting up Windows for Modem Connection to the Avaya S8xxx Server (Windows 2000 or XP) on page 548

- Configuring the remote PC for PPP modem connection (Windows 2000 or XP, Terminal Emulator, or ASA) on page 549

Once the Terminal Emulator is installed on your PC and you have a modem attached and configured to both your PC and the Avaya S8xxx Server, use the following steps to establish a modem connection to your Avaya S8xxx Server.

1. Double-click the Terminal Emulator icon off of your desktop. Alternatively, go to the Start menu, select **Programs**, then select **Avaya**, and finally select **Terminal Emulator**.

   The system displays the Terminal Emulator.

2. From the menu bar across the top of the screen, select **Phones**, then select **Connection List**.

   The system displays the Connections screen.

3. From the menu bar across the top, select **Connection**, then select **New Connection**.

   The system displays the Connection Settings screen.

4. Put in a name for the connection. Usually, this will be the name of your Avaya S8xxx Server.
5. In the Host window, click **Telnet**.
6. Click the **Emulation** tab at the top.

   The system displays the **Emulation** tab.

7. From the Emulator drop-down box, select the emulator you desire, usually 513BCT (default), AT&T 4410, AT&T or DECVT100.
8. In the Keyboard window, select **pbx**.
9. Click the **Modem** tab.

   The system displays the **Modem** tab.

10. In the **IP address** field, type the IP address of the connection **Dialup Status** box as noted in Step 9.
11. In the **TCP/IP port number** field, type **5023** to log in directly to the Communication Manager SAT command line.
12. In the **Modem** field, use the dropdown box to select the type of modem that your PC uses.
13. In the **Serial port** field, select the COM port you are using for your modem connection.
14. In the **Baud rate** field, select 9600 from the dropdown box.
15. Click the **Dial Numbers** tab.

    The system displays the **Display Numbers** tab.

16. Type the telephone number of the Avaya S8xxx Server as appropriate. Enter **1** in the **Country Code** field for long-distance.
17. Click **OK**.

18. On the Connections screen, double-click. the name of the connection you just set up.
19. The PC dials up the Avaya S8xxx Server, and when connected, the login prompt for the Communication Manager software appears.
20. Log in to Communication Manager to access the SAT command prompt screen.

Logging in to the Avaya S8xxx Server with ASA

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.

To use Avaya Site Administration, open the application and select the Avaya S8xxx Server you want to access. When prompted, log in.

When you are logged in, click **Start GEDI**.

Screen and command summary

The following screens are used to administer G700 Media Gateways, Avaya S8xxx Servers, and other media modules.

Media Gateways

The commands and screens for media gateways include:

The Media-Gateway administration screen is used to administer G700 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 G700 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 (LSP)** 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 Configuring the Local Survivable Processor on page 496 for details. This display-only field can be set only by the license file.
- Two additional fields in this section indicate if the primary call-processing controller is an S8300 Server. If traditional port networking is disabled and Processor Ethernet is enabled, an S8300 Server is controlling telecommunications.
  - **Port Network Support**: set to **n** indicates that traditional port networking is disabled. An S8300 Server is the primary call controller.
  - **Processor Ethernet**: set to **y** indicates the presence of an S8300 Server.

Quality of Service Monitoring

Several screen changes allow you to monitor Quality of Service (QoS) on an Avaya S8xxx Server with a G700 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 *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 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.
  1. Incoming LDN Extension
  2. Maximum Number of Trunks to Use for IGAR
  3. 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, which is as shown in Figure 80.

Figure 80: CM5.x IP Network Region IGAR/DPT Report

```
list ip-network-region igar-dpt                                        Page 1

                        IP NETWORK REGIONS - IGAR/DPT

                                                              LDN            Max
Region      Name                              Extension      Trks  DPT?  Location

 xxx   nnnnnnnnnnnnnnnnnnnn  xxxx-xxx-xxxx  xxx       n            xxx
 xxx   nnnnnnnnnnnnnnnnnnnn  xxxx-xxx-xxxx  xxx       n            xxx
 xxx   nnnnnnnnnnnnnnnnnnnn  xxxx-xxx-xxxx  xxx       n            xxx
 xxx   nnnnnnnnnnnnnnnnnnnn  xxxx-xxx-xxxx  xxx       n            xxx
```

Media Gateway serviceability commands

Additional commands related to media gateways appear in *Maintenance for the Avaya G700 Media Gateway controlled by an Avaya S8300 Media Server or an Avaya S8700 Media Server*. 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 on page 545. These include:
  - Message Sequence Trace (mst)
  - display errors
  - display alarms

Administering Voice or Network Statistics

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 upto 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 Manager Reports*, 555-233-505.

Administering SNMP

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 Administering traps on page 562.
- Administer an SNMP agent: For more information, see Administering SNMP agents on page 567.
- Administer a filter: For more information, see Administering filters on page 572.
- View the G3-Avaya-MIB: For more information, see Administering SNMP agents on page 567.
- 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** on page 562.

Turning on access for SNMP ports at the network level

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:

1. On the server's Server Administration Interface, click **Firewall** under the Security heading.

   The system displays the Firewall screen.
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, click the check boxes in both the **Input to Server** and **Output to Server** columns.
5. To save the changes, click **Submit**.

Administering traps

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

- Add a trap destination on page 562
- Displaying an administered trap on page 566
- Changing an administered trap on page 566
- Deleting an administered trap on page 567

Add a trap destination

Use the following steps to add a trap destination for SNMP.

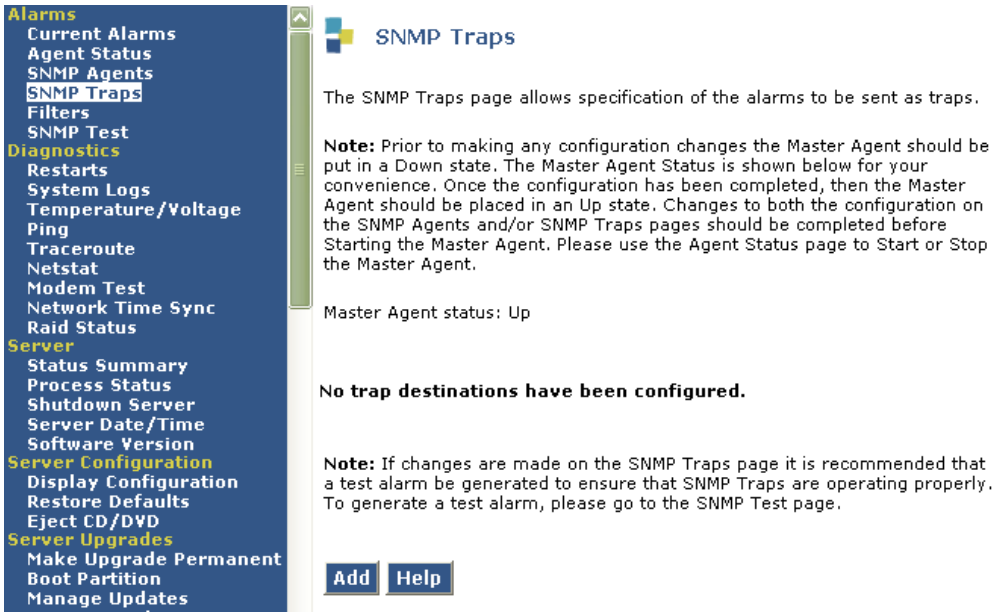
Instructions

To add a trap destination:

1. On the server's Server Administration interface, click **SNMP Traps** under the Alarms heading.

   The SNMP Trap screen appears as shown in example Figure 81.

Figure 81: SNMP Traps screen

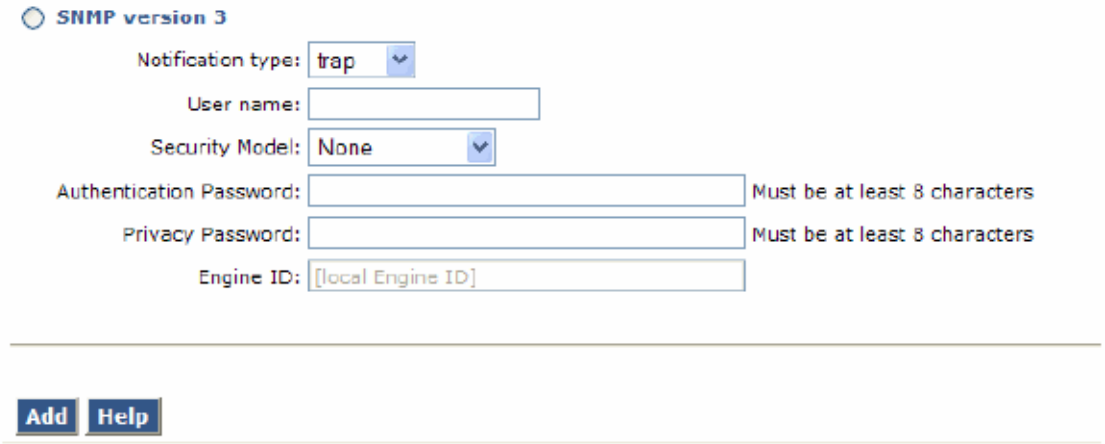


2. Check the status of the Master Agent.
   - If the status of the Master Agent is "Up": Select Agent Status from the navigation bar and click **Stop Agent**. Once the Master Agent is in a "Down" state, return to the SNMP Trap screen by clicking **SNMP Traps** on the navigation bar. If the status of the Master Agent is "Down," continue to step 3.
3. On the bottom of the screen, click **Add**.

   The **Add Trap Destination** screen appears as shown in Figure 82 and Figure 83.

Figure 82: Add Trap Destination screen

Figure 83: Add Trap Destination screen part 2



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.
6. Communication Manager supports SNMP v1, SNMP v2c, and SNMP v3. 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**:
     a. 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.
     b. In the **User name** field: Enter the SNMP user name that the destination recognizes.
     c. 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.
     d. **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: ’\ & , ‘ ".
     e. **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: ’\ & , ‘ ".
     f. **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.

   The SNMP Traps screen re-appears displaying 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.**

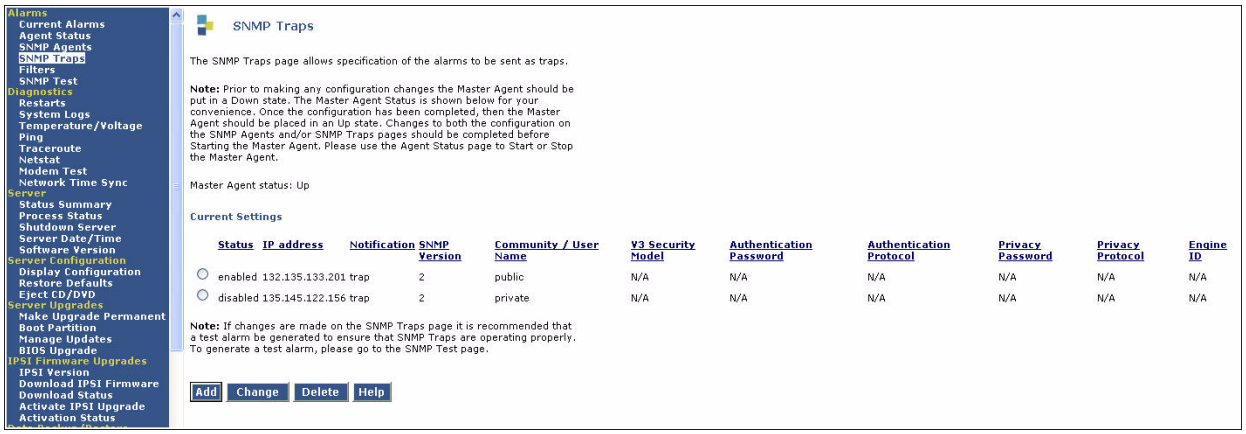
Displaying an administered trap

Use the following steps to display traps administered on the server:

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

   The SNMP Traps screen displays as shown in example Figure 84.

Figure 84: SNMP Traps screen after an addition



The administered traps display under the Current Settings heading.

Changing an administered trap

Use the following steps to change parameters on an administered trap:

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 is in 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.

   The Change Traps Destination screen appears.
4. Make the changes to the trap destination and click **Change**.

   The SNMP Traps screen appears displaying the changes made to the selected trap.
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 trap

Use the following steps to delete an administered trap:

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 is in 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.

   The Delete SNMP Trap Destination screen appears.
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.**

Administering SNMP agents

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 on page 562. For more information on how to check the status of the Master Agent, see step 2 under Instructions on page 568.

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.

Instructions

CAUTION:
On the S8700-Series Servers (duplicated servers), you must administer an SNMP agent exactly the same on both servers.

Use the following steps to administer an SNMP Agent:

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

   The SNMP Agents screen appears as shown in example Figure 85 and Figure 86.

Figure 85: SNMP Agents screen part 1

Figure 86: SNMP Agents screen part 2

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 is in 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:
   a. 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**:

a. **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.

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

c. **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.

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

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

  c. **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.

  a. **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.

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

c. **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.

d. **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.

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

f. **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.

g. **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.

Administering filters

Use the SNMP Filters screen to perform the following tasks:

- Adding a filter on page 572
- Changing a filter on page 577
- Deleting one or all filters on page 577
- Customer Alarm Reporting Options on page 577

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 Administering traps on page 562.

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 a filter

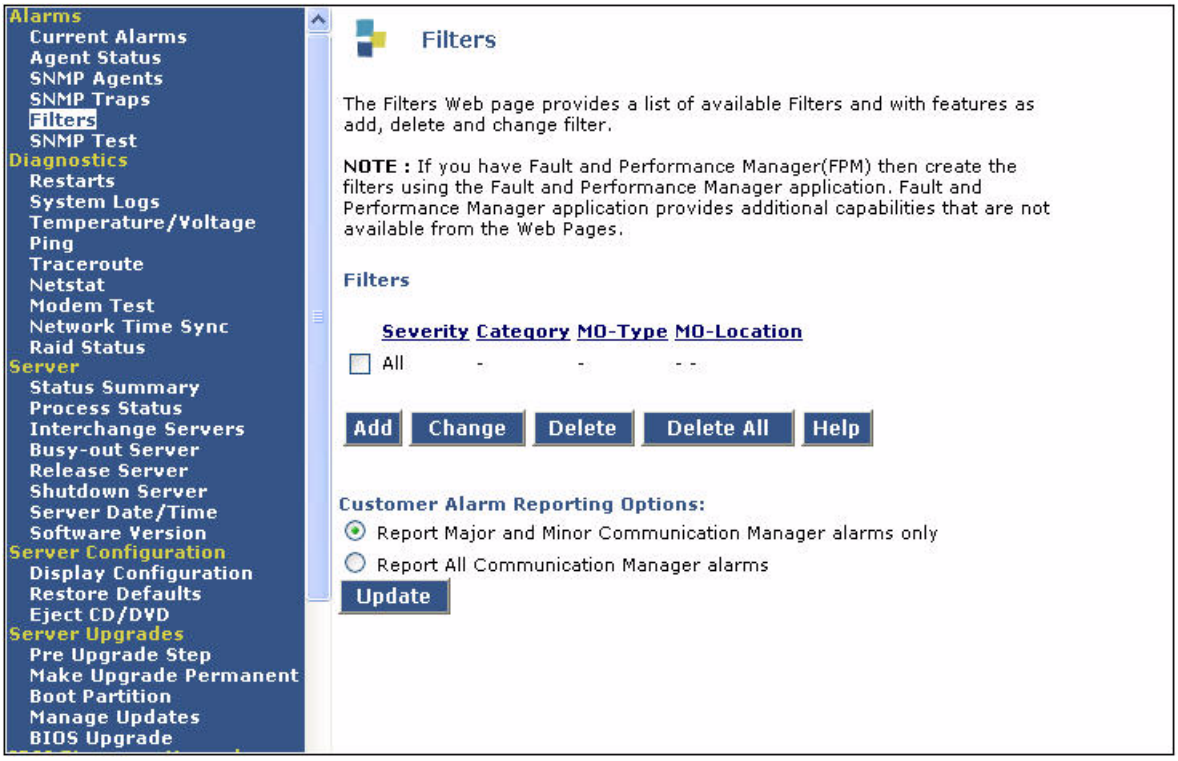
Use the following steps to add a filter.

Instructions

1. On the server's Server Administration Interface, click SNMP **Filters** under the Alarms heading.

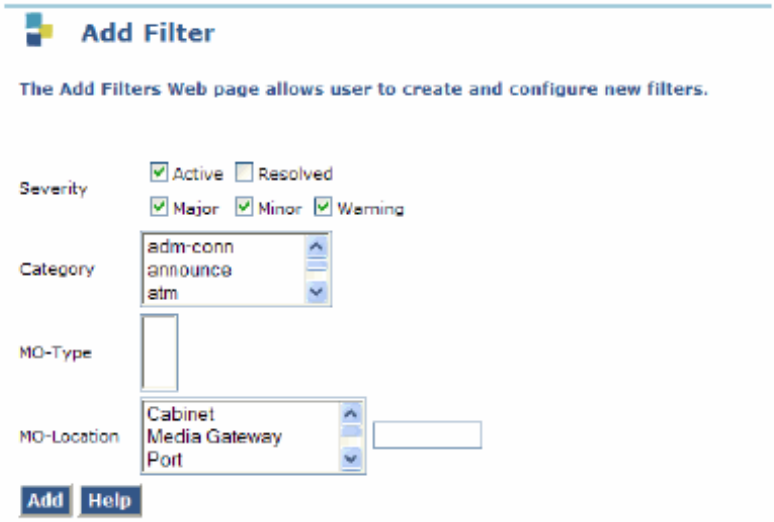
   The SNMP Filters screen appears as shown in example Figure 87.

Figure 87: SNMP Filters screen



2. Click **Add**. The Add Filter screen appears as shown in example Figure 88.

Figure 88: SNMP Filters screen - Add Filter



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 Table 11.

Table 11: 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

1 of 3

Table 11: Category with associated MO-Type table (continued)

Category	MO-Type
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
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
	2 of 3

Table 11: Category with associated MO-Type table (continued)

Category	MO-Type
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
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
	3 of 3

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 a filter

Use the following steps to change a filter:

1. From the server's Server Administration Interface, click SNMP **Filters** under the Alarms heading.

   The Filters screen appears.
2. Click the box associated with the filter you wish to change and press **Change**.

   The Change Filters screen appears.
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 filters

Use the following steps to delete one or all filters:

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

Use the following steps to set the **Customer Alarm Reporting Options**:

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

   The Filters screen appears displaying the selected reporting option.

Chapter 17: Collecting Call Information

Collecting Information About Calls

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.

Before you start

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).

Instructions

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.

1. Type **`change trunk-group n`**. Press **Enter**.

   The system displays the **Trunk Group** screen.

2. In the **CDR Reports** field, type **y**.

   This tells Communication Manager to create call records for calls made over this trunk group.

3. Press **Enter** to save your changes.

4. Type **`change system-parameters cdr`**. Press **Enter**.

   The system displays the CDR System Parameters screen.

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. 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.)

8. In the **Primary Output Ext.** field, type **2055**.

   This is the extension of the data module that we use to connect to our call accounting system.

9. In the **Record Outgoing Calls Only** field, type **n**.

   This tells Communication Manager to create records for both incoming and outgoing calls over all trunk groups that use CDR.

10. In the **Outg Trk Call Splitting** and **Inc Trk Call Splitting** fields, type **y**.

    This tells the system to create a separate record for any portion of an incoming or outgoing call that is transferred or conferenced.

11. In the **Outg Att Call Record** and **Inc Att Call Record** fields, type **y**.

    This tells the system to create a separate record for the attendant portion of any incoming or outgoing call.

More information

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, and these are described in the screens section of this book.

Related topics

For additional information on Call Detail Recording (CDR), see *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205.

Setting up Intra-switch CDR

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.

Instructions

In this example, we administer Communication Manager to record all calls to and from extensions 5100, 5101, and 5102.

1. Type ***change system-parameters cdr***. Press **Enter**.

   The system displays the CDR System Parameters screen.

2. In the **intra-switch CDR** field, type **y**.
3. Press **Enter** to save your changes.

4. Type **`change intra-switch-cdr`**. Press **Enter**.

   The system displays the Intra-Switch CDR screen.
5. In the first three available slots, type **5100**, **5101**, and **5102**.
6. Press **Enter** to save your changes.
7. Communication Manager will now produce call records for all calls to and from these extensions, including those that originated on the local server.

Related topics

See Intra-Switch CDR in *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, for more detailed information.

Tracking Calls by Account Code

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.

Instructions

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.

1. Type **`change system-parameters cdr`**. Press **Enter**.

   The system displays the **CDR System Parameters** screen.
2. In the **CDR Account Code Length** field, type **5**.
3. Press **Enter** to save your changes.
4. Assign an account button on the Station screen for extension 5004. See Adding Feature Buttons on page 105 for more information.
5. Provide your users with a list of account codes to use.
6. You can also assign a feature access code and give this to your users.

Forcing Users to Enter 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.

Before you start

Before you can administer Forced Entry of Account Codes, it must be enabled on the System Parameters Customer-Options **(Optional Features)** screens. If it is not, please contact your Avaya representative.

Instructions

In this example, we administer the system to force users in our North American office to enter an account code before making international calls.

1. Type **`change system-parameters cdr`**. Press **Enter**.

   The system displays the CDR System Parameters screen.
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**.
4. Press **Enter** to save your changes.
5. Type **`change toll 0`**. Press **Enter**.
6. The system displays the Toll Analysis screen.
7. In the first available **Dialed String** field, type **011**.

   This is the international access code for this office.
8. 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.
9. In the **Toll List** and **CDR FEAC** columns, type **x**.
10. Press **Enter** to save your changes.

More information

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.

Receiving Call-Charge Information

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.

Before you start

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

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.

1. Type **`change trunk-group 2`**.

   The system displays the ISDN Trunk Group screen with existing administration for this ISDN trunk group.

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, type **a**.
5. The **Charge Advice** field, type **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. Press **Enter** to save your changes.

Administering Charge Advice for QSIG trunks

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.

To administer charge advice for a trunk group with Supplementary Services Protocol **b***:*

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.

- 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

In this example, we will administer an existing Direct Inward and Outward Dialing (DIOD) trunk to receive PPM from the public network.

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, type **two-way**.
4. Click Next Page to find the **PPM** field.
5. In the **PPM** field, type **y**.
6. In the **Frequency** field, type **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.
8. Press **Enter** to save your changes.
9. 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.

Related topics

For more information about AOC and PPM, see Call Charge Information in *Avaya Aura™ Communication Manager Feature Description and Implementation,* 555-245-205.

Viewing Call Charge Information

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.

Instructions

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.

1. Type **`change trunk-group 2`**. Press **Enter**.
2. Click **Next Page** until you see the **Trunk Features** section.
3. In the **Charge Conversion** field, type **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, type **none**.
5. In the **Charge Type** field, type **Lira**.
6. Press **Enter** to save your changes.
7. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
8. In the **Charge Display Update Frequency (seconds)** field, type **30**.

   Frequent display updates might have considerable performance impact.
9. Press **Enter** to save your changes.
10. Now assign extension 5040 a **disp-chrg** button to give this user the ability to control the charge display. See Adding Feature Buttons on page 105 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.

Setting up Survivable CDR

The Survivable CDR feature is used to store CDR records to a server's hard disk. For ESS servers and LSPs, the Survivable CDR feature is used to store the CDR records generated from calls that occur when an LSP or ESS server is controlling one or more gateways or port networks. For a man 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 ESS servers that are Communication Manager 5.0 and later releases only. It is available on LSP platforms running Communication Manager 4.0 and later.

The CDR adjunct must poll each main, LSP, and ESS server regularly to see if there are any new data files to be collected. This is required even when an LSP or ESS server is not controlling a gateway or a port network because the CDR adjunct has no way of knowing if a LSP or ESS server is active.

The Survivable CDR feature utilizes the same CDR data file formats that are available with legacy CDR.

CDR files

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 CDR file naming convention on page 589). 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 an LSP or an ESS server, a new Current CDR file is created only if the LSP or the ESS server is controlling one or more gateways or port networks.

CDR file naming convention

The CDR data files have the following naming convention:

tssssss-cccc-YYMMDD-hh_mm

where:

- t is populated with an L for an LSP, an E for an ESS 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-'.

Removing CDR files

The CDR files can be removed by:

- The Survivable CDR feature: The Survivable CDR feature on the main, LSP, or ESS 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.

Access to CDR files

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.

High level administration

Use the following high level steps to administer the Survivable CDR feature:

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 on page 590).
2. Enable CDR storage on the hard disk (see Survivable CDR administration for the main server on page 592).
3. If using this feature on the main server: Administer the **Primary Output Endpoint** field on the main's **`change system-parameters cdr`** SAT screen to be **DISK** (see Survivable CDR administration for the main server on page 592). 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 an LSP and an ESS server: Administer the **Enable CDR Storage on Disk** field on the **`change survivable-processor`** screen (see Survivable CDR administration for an LSP or ESS server on page 592).

Detailed administration

Creating a new user account

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 LSP and/or ESS server when a filesync is performed.

To create a new user account:

1. On the server's Server Administration Interface, click **Administrator Accounts** under the Security heading.

   The Administrator Accounts page displays.

2. 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**.

   Administrator Logins -- Add Login page displays.

4. Enter the data in Table 12 in each field of the Administrator Logins -- Add Login page.

Table 12: 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
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
	1 of 2

Table 12: CDR adjunct user account recommended options (continued)

Field Name	Recommended Option
Number of days warning given before a password expires (PASS_WARN_AGE)	7
Days after password expires to lock account	-1
	2 of 2

5. Click **Add** to create the new user account.

Survivable CDR administration for the main server

Use the following steps to administer the Survivable CDR feature for a main server:

1. On page 1 of the CDR System Parameters screen:
   a. **Enable CDR Storage on Disk?**: Possible entries for this field are yes or no. Entering yes (**y**) in this field enables the Survivable CDR feature for the main, LSP, and ESS servers. If this field is set to no (**n**), 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.

      For information about the CDR System Parameters screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Survivable CDR administration for an LSP or ESS server

Use the following steps to administer the Survivable CDR feature for an LSP or an ESS server:

Note:
The Survivable CDR feature is administered on the main server for the LSP and ESS servers.

Important:
An LSP or ESS 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.

1. On the CDR System Parameters 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, LSP, and ESS servers. If this field is set to no, the CDR functionality remains legacy CDR.

2. Survivable Processor - IP-Services screen, page 3:
   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 LSP or ESS server. When the **Service Type** field is set to **CDR1** or **CDR2** and the **Store to Dsk** field is set to **y**, all CDR data for the specific LSP or ESS server being administered will be sent to the hard disk rather than output to an IP link. LSP or ESS servers will only store CDR records to hard disk when the LSP or ESS server is controlling a gateway or port network.

Important:
You must complete the Survivable Processor - IP Services screen for ***each*** LSP or ESS server that will utilize the Survivable CDR feature.

Note:
The **Enable** field for a given line in the Survivable Processor - IP Services screen must be set to **o** (overwrite) to allow changes for that row.

Chapter 18: Administering LDAP Directory Application

Overview

The LDAP Directory Application is available from the Administration menu in the System Management Interface. The LDAP Directory Application is a part of Communication Manager and is installed with Avaya S8300D, S8500C, S8510, S8720, and S8730 Servers, while installing or upgrading to Avaya Aura™ Communication Manager Release 5.2.

You can use the LDAP Directory Application to search an LDAP database using browsers on your compatible 46xx and 96xx phones. You can use the LDAP Directory Application web pages to configure the LDAP Directory Application to connect to an LDAP database and to customize the user search experience.

Configuring the LDAP Directory Service

You must configure the LDAP Directory Application correctly for the WML Browsers to perform search operations.

To configure the LDAP Directory application:

1. Go to **System Management Interface** > **Administration** > **Directory Application** to launch LDAP Directory Application.
2. Specify the LDAP connection settings on the **General Settings** web page.
3. Click **Test Connection** to ensure that the Directory Application is connecting to the LDAP database.
4. Enable the Directory Application for HTTP or HTTPS traffic.
5. (Optional) Use the **Search Screen Settings** web page to customize the Search screen on the phone browser.
6. (Optional) Use and the **Details Screen Settings** web page to customize the **Details** screen on the phone browser.

Synchronizing Communication Manager station with the LDAP Directory

You can use the Avaya Site Administration **Export to LDAP directory** capability to export data from the applicable station fields to your LDAP database. The Avaya Site Administration tool also provides a scheduling feature for the export.

Configuring the 46xx and 96xx phones

Configure the URL on compatible 46xx and 96xx phones using the WMLHOME property in the settings file.

The URL for HTTP is: http://<CM IP Address/Host Name>/directoryclient/search.php

The URL for HTTPS is: https://<CM IP Address/Host Name>/directoryclient/search.php

For more information about configuring the WML Browsers, see *4600 Series IP Telephone LAN Administrator Guide* and *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide*.

Index

Numerical

2420/2410 DCP telephone, downloading firmware . . 100
302D console 152
7400A data module 466
7400B+ data module 466
7400C High Speed Link 467
7400D data module 467
7500 data module 465, 467
8400B data module 466

A

AAA services
administering 26
abbreviated dialing
adding lists 131
feature button 109
fixing problems 133
program feature button 108
special character feature button 109
abbreviated ring feature button 109
access endpoints
administered connection 469
Access Security Gateway (ASG)
description 391
logging in with 23
access trunks 414
account codes
forcing users to enter 583
tracking calls 582
account feature button 110
ACD, see Automatic Call Distribution (ACD)
ACTR, see Automatic Customer Telephone Rearrangement
adjuncts
AESVCS 522
CDR 522
CMS 521
with Processor Ethernet 521
Adjunct-Switch Applications Interface, see CallVisor Adjunct-Switch Applications Interface (ASAI)
administered connections (AC) 468
access endpoints 469
administering 471
alarm feature button 109
detailed description 468
dropping 470
establishing 469
failures 470
typical applications 469
Administering Avaya Aura™ Communication Manager
admonishments 12
chapter summaries 10
commenting on 15
conventions 11
overview 9
related resources 13
trademarks 13
administering LDAP Directory application 595
administering main/LSP split registration 523
administration procedures 526
considerations 525
detailed description 523
implementation procedures 526
Administering Voice or Network Statistics 559
administrable Alternate Gatekeeper List (AGL) . . . 528
administration procedures 539
building AGL lists 530
considerations 538
load balancing 529
troubleshooting scenarios 541
verify AGL settings for stations 540
Administrable Language Displays, changing 168
administration feature button 110
Advice of Charge (AOC) 584
AESVCS, with Processor Ethernet 522
after call work mode feature button 110
alarms
major alarm feature button 121
minor/major alarms feature button 123
off-board feature button 124
alert agent feature button 110
alias, adding telephones using 76
alphanumeric dialing 458
Alternate Facility Restriction Levels (AFRL) feature button 110
Alternate Gatekeeper List (AGL) 523
AMET (Avaya Message Editing Tool) 170
analog telephones 71
ANI, displaying calling party information 167
announcement data module 465
announcements
locally sourced 53
overview 433
playing in vector 234
using the VAL or G700 v VAL 433
answer detection, administering 426

Answer Supervision 363
answerback paging 444
Application Enablement Services (AESVCS), with Processor Ethernet 522
area codes
adding 261
restricted 253
ASA,see Avaya Site Administration (ASA)
ASAI, see CallVisor Adjunct-Switch Applications (ASAI) Interface
ASG, see Access Security Gateway (ASG)
assistance feature button 110
asynchronous data module 467
attendant
Attendant Backup Alerting 164
Attendant Direct Trunk Group Selection button . . 156
Attendant Overflow Timer 165
crisis alert feature button 116
queue calls feature button 111
queue time feature button 111
Return Call to (same) Attendant 165
attendant consoles
302 149
adding 154
Avaya PC 153
description 149
feature buttons 155
managing 149
providing backup 164
removing 163
setting parameters 162
SoftConsole IP Attendant 153
audio group, adding 54
Audix One-Step Recording feature button 111
authorization codes
creating 264
security violation feature button 110
setting up 392
using to override call restrictions 263
autodial feature button 112
auto-in mode feature button 112
Automatic Alternate Routing (AAR) 247
automatic answer intercom calls 447
Automatic Call Distribution (ACD)
description 245
stroke count feature button 128
automatic callback
feature button 111
if extension is busy 61
with 4601 and 4602 IP 93
automatic circuit assurance feature button 109
Automatic Customer Telephone Rearrangement, moving telephones using 79
automatic hold 61
automatic intercom feature button 111
automatic message waiting feature button 111
Automatic Number Identification (ANI) feature button . 110
Automatic Route Selection (ARS)
allow local information calls 255
analysis. 250
assigning ARS FAC 248
displaying analysis information 249
inter-exchange carrier calls (IXC) 253
operator assisted calls 252
overriding call restrictions 263
partitioning 264
restricted area codes 253
restricting calls 262
automatic routing
feature access code (FAC) 247
time of day (TOD) 267
automatic wakeup
feature button 112
printer alarm feature button 125
aux work feature button 112
Avaya documentation
commenting on 15
obtaining Avaya books on the Web 14
Avaya IP Agent 88
Avaya Message Editing Tool (AMET) 170
Avaya S8XXX Servers
accessing 18
accessing web interface 498
administering 493, 498
call processing 544
Local Survivable Processor configuration 496
SNMP agents 561
Avaya Site Administration (ASA)
adding a new switch 22
adding a new voice system 22
configuring 22
downloading from Web interface 20
installing 20
overview 20
starting 21
using to access Communication Manager 545
Avaya Terminal Emulator
using for LAN connection 553
using for modem connection 554
Avaya Video Telephony Solution 297
administering 298
description 297

B

backups
performing 40
saving translations. 38
bandwidth, setting limits on WAN 50
barrier codes 331
billing information, collecting. 579

blocking, prevention 488
bridged call appearance
analog phone feature button 109
creating 135
feature button 112
setting up 135
bulletin board 36
deleting messages 37
displaying messages 37
posting messages 37
busy indicator feature button 113
busy verification
feature button 129
using. 391
button view feature button 113
buttons
directory 178
feature 105
help 11

C

call appearance feature button 113
call charge information
administering Advise of Charge 584
administering Periodic Pulse Metering (PPM). . . 586
collecting information about calls. 579
Periodic Pulse Metering (PPM) 584
receiving 584
viewing. 587
call coverage
adding to a coverage path. 188
administering system-wide characteristics 183
advanced 186
assigning coverage paths 185
bridging onto call gone to coverage 61
call forwarding 190
calls redirected to external numbers 187
coverage answer groups 189
defining time-of-day coverage 188
redirecting off-net 186
setting up 183
time-of-day coverage plan. 189
call detail recording (CDR)
alarm feature button 114
collecting information about calls. 579
establishing 580
forced entry of account codes (FEAC) 583
Intra-switch CDR 579
intraswitch CDR 581
PCOL trunks 413
with Processor Ethernet. 522
call display feature button 113
call forwarding
busy/don't answer feature button 114
Enhanced Call Forwarding 194
feature button 113
setting up 190, 192, 370
call park feature button 113
call pickup 209
adding pickup groups 212
alerting 210, 213
assigning button. 214
assigning FAC 215
changing button 217
deleting pickup groups. 215, 216
directed. 223
creating COR for 224
removing 227
extended pickup groups 217
changing 223
flexible 220
feature button 114
pickup numbers 219
removing button. 217
setting up 212
call pickup alerting
enabling 214
call processing
accessing Communication Manager 544
administering 544
call restrictions, overriding. 263
call routing, modifying. 260
call timer feature button 114
call work code feature button 131
caller information
ANI. 167
displaying. 167
displaying Incoming Call Line Identification (ICLID) 168
feature button 114
calling party number (CPN)
CPN block feature button 115
CPN unblock feature button 116
calling privileges, managing 247
calls
data setup 451
handling incoming 183
observing 448
operator assisted 252
overriding restrictions 263
recording 581
redirecting off-net 186
routing outgoing 247
tracking. 582
CallVisor Adjunct-Switch Applications Interface (ASAI) 490
description 490
setting up 492
CAS backup feature button 114
check in feature button 114
check out feature button 115

chime paging
assigning chime codes . . . 441
fixing problems . . . 441
setting up . . . 439
circuit packs
configuration . . . 41
universal digital signaling level 1 . . . 482
class of restriction (COR)
changing . . . 248
changing with feature access code . . . 63
strategies for assigning . . . 62
class of service (COS), overview . . . 48
clocked manual override feature button . . . 115
CMS
survivable . . . 521
with Processor Ethernet . . . 521
CO attendant feature button . . . 123
CO trunks . . . 407
command line interface (CLI)
accessing . . . 546
using Avaya Terminal Emulator . . . 553
using SSH . . . 546
using Telnet . . . 548
conference display feature button . . . 115
configure 46xx and 96xx phones using the WMLHOME property . . . 596
console parameters, setting . . . 162
consult feature button . . . 115
control of IP telephone mode . . . 89
COR, see class of restriction (COR)
COS, see class of service (COS)
coverage answer group
adding . . . 189
extensions with call forwarding activated . . . 191
coverage callback feature button . . . 115
Coverage of Calls Redirected Off Net (CCRON) . . . 363
coverage options, assigning . . . 372
coverage path
assigning to users . . . 185
creating . . . 184
crisis alert feature button . . . 116

D

data calls
characters used . . . 453
overview . . . 451
setup . . . 451
data connection types . . . 451
data extension feature button . . . 116
data hotline . . . 459
data line data module . . . 465
data modules
7400A . . . 466
7400B+ . . . 466
7400C High Speed Link . . . 467
7400D . . . 467
7500 . . . 465, 467
8400B . . . 466
announcement . . . 465
asynchronous . . . 467
BRI . . . 465
data line . . . 465
DCP
data-terminal dialing . . . 455
telephone dialing . . . 456
detailed description . . . 466
Ethernet . . . 465
ISDN-BRI . . . 456
PPP . . . 465
processor/trunk . . . 465
types . . . 465
data privacy, administering . . . 460
data restriction . . . 462
data restriction, administering . . . 463
data terminal (keyboard) dialing
alphanumeric . . . 458
default dialing . . . 462
ISDN-BRI data modules . . . 456
data-only off-premises extensions . . . 464
date and time
displaying . . . 36
feature button . . . 116
setting for system . . . 34
daylight savings rules
displaying . . . 27
establishing . . . 26
DCP data modules . . . 455
default dialing . . . 462
delayed ring feature button . . . 109
delete message feature button . . . 116
denied calls, rerouting . . . 52
Device Manager
accessing from a web browser . . . 497
accessing through Network Management Console with VoIP SystemView . . . 497
using to administer G700 components . . . 497
dial access codes . . . 43
dial intercom feature button . . . 116
dial plan
adding extension ranges to . . . 44
adding feature access codes to . . . 46
changing feature access codes in . . . 47
displaying . . . 43
modifying . . . 44
multi-location . . . 45
overview . . . 42
prepending location prefix . . . 45
uniform . . . 44
Dial Plan Analysis Table
overview . . . 42

Dial Plan Transparency (DPT)
administering . . . 47
dial tone, special . . . 62
dialing
alphanumeric . . . 458
default . . . 462
DID trunks . . . 410
DID view button . . . 116
digital trunks . . . 416
digits
absorbing . . . 423
inserting . . . 423
DIOD trunks . . . 416
direct inward dialing (DID)
DID view feature button . . . 116
directed call pickup . . . 223
creating COR . . . 224
removing . . . 227
directed call pickup feature button . . . 117
directory assistance feature button . . . 123
directory buttons . . . 178
directory feature button . . . 117
directory, integrated
hiding names . . . 178, 179
telephone feature button . . . 117
display charge feature button . . . 117
display language, changing . . . 168
display messages in additional languages
standard telephone features . . . 179
displays
administering for QSIG trunks . . . 177, 431
for QSIG trunks . . . 177, 431
managing . . . 167
distinctive ringing . . . 62
do not disturb feature buttons
extension . . . 119
group . . . 119
individual . . . 118
downloading firmware . . . 100
drop feature button . . . 118
DS1 trunk service
enhanced administration . . . 419
recommended T1 settings . . . 418
screen and field guidelines . . . 419
setting up . . . 416
duplicate command (telephone) . . . 75
duplicating telephones . . . 75

E

emergency
notifying digital pager . . . 59
receiving notification . . . 57
EMU, see Enterprise Mobility User (EMU)
endpoints, *see* telephones
Enhanced Call Forwarding . . . 194
Enhanced Call Transfer (ECT) . . . 383
enhanced redirection notification
enabling . . . 200
Enterprise Mobility User (EMU)
activating from visited telephone . . . 146
configuring system for . . . 144
deactivating . . . 146
defining calling party identification options . . . 145
setting options for stations . . . 145
setting up . . . 143
system requirements . . . 143
Ethernet data module . . . 465
exclusion feature button . . . 118
Export to LDAP directory . . . 596
extended pickup groups
changing . . . 223
setting up . . . 217
extender passwords, assigning . . . 368
extension ranges, adding to dial plan . . . 44
Extension to Cellular . . . 137
screens used to administer . . . 138
setting up feature access button for . . . 139
Extension to Cellular feature access button . . . 119
extensions (ext) . . . 72
extensions, data-only . . . 464

F

FAC, see feature access code (FAC)
Facility Restriction Level (FRL) . . . 247
facility test call alarm feature button . . . 128
far end mute for conf feature button . . . 119
fax
adding . . . 86
enabling transmission over IP networks . . . 553
over IP network . . . 87
feature access code (FAC)
adding to dial plan . . . 46
ARS . . . 248
changing on dial plans . . . 47
feature buttons
adding . . . 105
attendant console . . . 155
enabling extended text fields for . . . 107
feature buttons table . . . 108
increasing text field length . . . 106
restricting customization of types . . . 107
Feature Name . . . 297
administering
prerequisites . . . 298
firmware
disabling downloads . . . 103
displaying download status . . . 103
downloading to 2420/2410 DCP telephone . . . 100

downloading to a single station 101
downloading to multiple stations 102
firmware video compatibility matrix 308
flash feature button 119
FX trunks 407

G

G700 Media Gateway
administering 493
media module description 495
physical design 493
security considerations 545
using Device Manager 497
G700 Virtual Val 433
glare, prevention 487
go to cover feature button 119
group communications 437
automatic answer intercom calls 447
chime paging over loudspeakers 439
paging over speakerphones 442
voice paging over loudspeakers 437
whisper paging 444
group do not disturb feature button 119
group page feature button 119

H

H.320 calls 310
h.323 softphone
using single telephone 90
H.323 stand-alone mode 88
H0 channels 486
H11 channels 485
H12 channels 486
Hayes command set 467
headset feature button 120
help
buttons 11
numbers to call 15
hold, automatic 61
home equipment, installing 373
hot desking enhancement 402
Personal Station Access (PSA) 402
station lock 402
telephones 403
hotline, data 459
hunt groups
adding announcements 231
changing 229
night service 207
night service feature button 120
overview 227
setting up 227
setting up a queue 229

I

ICLID, see Incoming Call Line Identification
immediate manual override feature button 122
Improved port network recovery from control network outages 542
incoming call identification feature button 120
Incoming Call Line Identification (ICLID) 168
inspect mode feature button 120
integrated directory
hiding names 117, 178, 179
telephone feature button 117
Integrated Management
main screen 500, 501
intercom
automatic answer calls 447
automatic intercom feature button 111
dial intercom feature button 116
using telephone as 445
Inter-Exchange Carrier (IXC) codes 253
internal automatic answer feature button 120
international modem settings 551
Intra-switch CDR 579
invalid calls, rerouting 52
IP softphone 88
fixing problems 91
using road-warrior mode 90
using telecommuter mode 91
IP telephones
adding 92
changing from dual-connect to single-connect . . . 93
ISDN
collecting call charge information 584
ISDN-BRI data modules 456
ISDN-PRI terminal adapters 481
ISDN trunk groups, administering 427
IXC, see Inter-Exchange Carrier (IXC) codes

L

language display, changing 168
last number dialed feature button 120
LDAP Directory Application
administering 595
configuring 595
synchronizing 596
leave word calling
cancel feature button 121
lock feature button 121
store feature button 121
license-error feature button 120
link alarm feature button 121
Listed Directory Number (LDN), administering . . . 424
load balancing 522

local feature button . . . 117
Local Survivable Processor (LSP) . . . 496
locally sourced announcements and music . . . 53
adding an audio group . . . 54
adding Music-on-Hold group . . . 54
location prefix, prepending . . . 45
locations
by region . . . 269
multiple . . . 256
routing . . . 258
logging in . . . 17
for remote administration . . . 17
from system terminal . . . 17
remotely over the network . . . 19
using Avaya Site Administration (ASA) . . . 20
with Access Security Gateway . . . 23
logging off . . . 25
login security violation notification (SVN) feature button 121
logins
adding . . . 391
administering . . . 26
system security . . . 384

M

main/LSP split registration
administering . . . 523
administration procedures . . . 526
considerations . . . 525
detailed description . . . 523
implementation procedures . . . 526
major alarm feature button . . . 121
malicious call trace
MCT activation feature button . . . 122
MCT control feature button . . . 122
manual message waiting feature button . . . 121
manual override . . . 115
manual-in mode button feature button . . . 122
media gateway, G700 . . . 493
message line . . . 12
message retrieval feature button . . . 115, 123
message waiting
activation feature button . . . 123
deactivation feature button . . . 124
feature button . . . 111
messages
delete message feature button . . . 116
deleting from bulletin board . . . 37
displaying on bulletin board . . . 37
posting on bulletin board . . . 37
minor/major alarms feature button . . . 123
modem pooling
administering . . . 474
overview . . . 474
modems
adding . . . 86
configuring remote PC for PPP modem connection 549
enabling transmission over IP networks . . . 553
international settings . . . 551
over IP network . . . 87
setting up windows for modem connection to server 548
using Windows for PPP modem connection . . . 550
multi-location dial plan . . . 45
Multimedia Applications Server Interface (MASI) feature
AAR and ARS . . . 290
administering . . . 278
autonomous MMCX features . . . 271
basic features not supported . . . 293
Call Center features not supported . . . 293
Call Detail Recording (CDR) . . . 290
call redirection . . . 291
command permissions . . . 290
conferencing . . . 292
configurations . . . 274
description . . . 271
features not supported . . . 293
planning . . . 273
status tracking, terminals and trunk . . . 292
terms . . . 272
transferring . . . 292
troubleshooting . . . 296
trunk groups . . . 292
voice messaging access . . . 291
Multimedia Call Handling (MMCH) feature . . . 309
1-number access . . . 325, 342
authorization . . . 331
call association (routing) . . . 338, 355
call redirection . . . 332
conferencing . . . 332
list commands . . . 360
monitoring commands . . . 359
multimedia complexes . . . 310
status commands . . . 359
multimedia calling . . . 271
multimedia complex
basic . . . 310
enhanced . . . 311
enhanced mode . . . 341
multimedia feature buttons
mm basic mode . . . 123
mm call . . . 123
mm call forward . . . 123
mm data conference . . . 123
mm multi-number . . . 123
mm PC audio . . . 123
multiple locations
routing with . . . 258
setting up . . . 256
music
adding audio group . . . 54

locally sourced 53
Music-on-Hold (MOH)
adding Music-on-Hold group. 54
providing for multiple tenants 55
setting up 53

N

N x DS0 channels 486
network regions, WAN bandwidth limits 50
next feature button 124
night service
activate feature button 124
description 201
for hunt groups 207
for trunk groups. 207
hunt group feature button 120
setting up trunk answer from any station (TAAS) . 205
trunk group button 129
no hold conference feature button. 124
normal call identification feature button 124
normal feature button 117

O

observing calls. 448
off-premises extensions, ... 464
operator assisted calls 252
outgoing calls, routing 247

P

paging
chime paging 439
over speakerphone 442
users who are on active calls 444
voice paging over loudspeakers 437
whisper paging 444
partitioning, ARS. 264
passwords
adding 391
encryption 383
extender 368
PC Interface security 478
PCOL trunks. 411
Periodic Pulse Metering (PPM) 584, 586
personal CO line feature button 124
Personal Station Access (PSA)
setting up 365
telecommuting 363
pickup groups
deleting 215, 216
deleting user 215
extended 217
flexible 220
listing extended pickup groups 216
pickup numbers 219
Point-to-Point Protocol data module 465
port address 41, 71
port network (PN) preferential trunk routing. 485
PPM, see Periodic Pulse Metering (PPM)
PPP
data module 465
modem connection 549, 550
prefixes, adding 262
PRI endpoints, wideband switching 482
print messages feature button 125
priority calling feature button 125
Processor Ethernet (PE)
administering in Communication Manager. . . . 520
AESVCS 522
call detail recording 522
configuring an LSP or an ESS server 518
configuring PE Interface 513
defining network port usage 511
duplicated server 508
high-level steps to setting up 509
load balancing 522
overview 508
setting Alternate Gatekeeper List (AGL) priorities 523
processor/trunk data module (P/TDM) 465
property management system (PMS)
PMS failure feature button 124
printer alarm feature button 125

Q

queue calls feature button. 125
queue time feature button 125

R

redial feature button 120
redirection on no answer feature button 124
release agent feature button. 125
remote access
disabling 401
disabling permanently 377
enabling 401
security violation feature button. 126
setting up 375, 376
remote access barrier code security violation notification call feature button. 126
remote administration, logging in 17
remote office
adding a node. 97
adding telephones. 99
assigning network regions 99
setting up 96

setting up trunk groups 97
restricting
area codes 253
calls 62
outgoing calls. 262
ringer cutoff feature button 125
ringing, assigning 136
road-warrior mode, using 90
routing
based on time of day 235
changing 261
modifying call. 260
outgoing calls. 247
overview 247
time of day routing 267

S

S8300 Media Server
screens and commands 556
S8300 Server
faceplate 494
S87XX series media server
logging in remotely over the network 19
SAT, see System Access Terminal (SAT)
screens, *see* screens *under individual feature names*
script tags and abbreviations 174
scroll feature button 126
Secure Shell (SSH), using for remote login 546
security 383
checklist 386
disabling remote access. 401
enabling remote access 401
enhanced call transfers (ECT) 383
for G700 Media Gateway 545
logins 384
passwords 383
physical 383, 386
preventing toll fraud. 384
securing trunks 383
Security Violations Notification (SVN) 383
setting up authorization codes 392
security violation feature button 110, 121
Security Violations Notification (SVN) 383
responses 401
setting up 395
send all calls
feature button 126
TEG feature button 126
servers
accessing 18
accessing web interface. 498
administering 493, 498
call processing 544
Local Survivable Processor configuration. 496
SNMP agents 561
service observing feature button 126
service observing, setting up 448
signal feature button 127
Simple Network Management Protocol, see SNMP
single connect h.323 softphone, using 90
slot address 41
SNMP
administering 507, 561
speakerphone, paging over 442
special dial tone 62
speed dialing, see abbreviated dialing
stand-alone H.323 mode 88
standard telephone features
display messages in additional languages. 179
Station Lock
screens 66, 400
COR 66
Feature Access Code (FAC) 66, 400
station lock
description 64
feature button 127
feature interactions 65
using 397
station security code 180
creating. 367
end-user administration 180
exception handling 181
violation referral feature button 127
stations, adding 70
stations, *see* telephones
status line 12
stored number feature button 127
stroke count feature button 128
survivable CMS 521
switches, adding in ASA 22
switching, wideband 479
Synchronizing LDAP Directory. 596
System Access Terminal (SAT) 545
system administration
basics 17
changing system parameters. 49
displaying system date and time 36
establishing daylight savings rules 26
logging in 17
logging off 25
planning 41
security 383
setting system date and time 34
setting time of day clock synchronization 28
system -wide settings 49
treatment for denied or invalid calls 52
using Avaya Site Administration 20
system parameters, changing 49
system printer alarm feature button 125

system reset alert feature button 126
system security, see security
system-wide settings 49

T

T.120 calls 310
T1 418
T1, recommended settings for digital trunks 418
TAAS (trunk answer from any station) 205
telecommuter mode, using 91
telecommuting
  Answer Supervision 363
  assigning coverage options 372
  associating office phone number to home station . 374
  changing settings 378
  configuring Communication Manager for 363
  Coverage of Calls Redirected Off Net (CCRON) . 363
  disassociating home stations 374
  installing home equipment 373
  Personal Station Access 363
  setting up 363
telephone dialing
  data call preindication 456
  DCP data modules 456
  one-button transfer to data 456
  return-to-voice 456
telephone feature buttons table 108
telephones
  adding 70
    IP softphone 88
    IP telephone 92
    using an alias 76
  adding using templates 75
  analog 71, 136
  associating office number to home station 374
  customizing 77
  digital 136
  disassociating home stations 374
  duplicating 75
  extension 72
  feature buttons table 108
  installing new 69
  IP softphones 88
  IP telephones
    adding 92
  managing 69
  managing displays 167
  managing features 105
  moving with ACTR 79
  moving with TTI 81
  physically connecting 72
  removing 85
  swapping 78
  upgrading 78
  use of term 11
  using ACTR to move 79
  using as intercoms 445
Telnet
  turning off for increased security 548
  using over the Customer LAN 548
tenant partitioning, MOH for multiple tenants 55
Terminal Self Administration (TSA)
  assigning a security code 141
  fixing problems 142
  setting up 140
Terminal Translation Initialization (TTI) 79
  fixing problems 84
  moving telephones using 81
terminating extension group (TEG)
  assigning 245
  feature button 128
tie trunks 414
time and date
  displaying 36
  feature button 116
  setting for system 34
time of day clock synchronization 28
time of day coverage 188
time of day routing
  override button 115
  setting up 267
timer feature button 128
toggle-swap feature button 128
toll fraud, preventing 384
translations
  copy protection 38
  problems with saving 40
  saving 38
trunk answer from any station (TAAS) 205
trunk feature buttons
  ID 129
  night service 129
  trunk name 129
trunk flash feature button 119
trunk group night service button 129
trunk groups
  access trunks 414
  adding trunks 420
  administering Listed Directory Numbers 424
  CO trunks 407
  DID trunks 410
  digital trunks 416
    enhanced DS1 administration 419
  FX trunks 407
  inserting and absorbing digits 423
  ISDN trunks 427
  night service 207
  overview 405
  PCOL trunks 411

call detail recording 413
port network (PN) preferential trunk routing 485
removing 421
resetting 422
restrictions 413
tie trunks 414
tips for working with 405
WATS trunks 407
TTI, see Terminal Translation Initialization

U

Unicode, administering display 170
uniform dial plan 44
universal digital signaling level 1 circuit pack 482
upgrading telephones 78
user profiles
administering 26
UUI-info feature button 129

V

VAL, getting started 433
VDN of origin announcement feature button 130
VDN, see Vector Directory Number (VDN)
Vector Directory Number (VDN)
adding 243
overview 232, 243
viewing 244
vectors
allowing callers to leave messages 236
caller options 237
deleting a step 239
fixing problems 242
inserting a step 238
overview 232
playing an announcement 234
queueing calls 234
redirecting calls 236
routing based on time of day 235
variables in vectors 239
video conferencing 310
VIP feature buttons
check-in 129
retry 129
wakeup 129
Virtual VAL (v VAL), getting started 433
Voice or Network Statistics
administering 559
voice paging over loudspeakers
fixing problems 438
setting up 437
voice terminals, *see* telephones
VuStats feature button 130

W

WAN, setting bandwidth limits 50
warning
for users if their calls are redirected 62
when telephones are off-hook 62
WATS trunks 407
Web interface tasks
backing up and restoring data 502
copying files to the server 503
SNMP administering 507
upgrading software and configuration 503
whisper paging 444
activation feature button 130
administering 444
answerback feature button 130
deactivate feature button 131
wideband switching 479
access endpoint 483
administering 488
blocking prevention 488
channel allocation 480
channel service unit 482
data backup connection 483
data service unit 482
direction of trunk/hunting within facilities 485
endpoint applications 481
facility lists 484
glare prevention 487
H0 channels 486
H11channels 485
H12 channels 486
ISDN-PRI terminal adapters 481
ISDN-PRI trunk groups and channel allocation . 484
line-side (T1 or E1) facility 482
N x DS0 channels 486
networking 484
port network (PN) preferential trunk routing . . . 485
PRI-endpoints 482
primary data connectivity 484
scheduled batch processing 483
typical uses 480
universal digital signaling level 1 circuit pack . . 482
work code feature code 131
World Class Routing 247