Administering Avaya Aura® Communication Manager

Release 8.1.x
Issue 14
December 2022

Notice

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

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time as indicated in the order, Documentation, or as authorized by Avaya in writing. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). End User may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below);

or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

Contents

Chapter 1: Introduction

Avaya Aura® Communication Manager is the centerpiece of Avaya applications. Communication Manager runs on a variety of S8300E, and other Avaya common servers and provides control to Avaya Branch Gateway and Avaya communications devices.

Communication Manager 8.1.x can be deployed on a Avaya Solutions Platform (ASP) 120 and 130 servers, Common Server R2 and R3, S8300E and a customer provided VMware environment. The above platforms provides control to Avaya Branch Gateway and Avaya communication devices. Communication Manager can be designed to operate in either a distributed or a networked call-processing environment.

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.

Communication Manager carries forward all the current DEFINITY® capabilities of the customer. Communication Manageralso offers enhancements that customers can use to take advantage of new distributed technologies, increased scalability, and redundancy. Communication Manager evolved from DEFINITY® software and delivers no-compromise, enterprise IP solutions.

For more information, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Purpose

This book describes the procedures and screens used in administering Communication Manager that runs on any of the following:

- Avaya servers, HP ProLiant DL360p G8, HP ProLiant DL360 G9, and Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630.
- Avaya servers configured as a Survivable remote server, S8300E, Avaya Solutions Platform (ASP) 120 and 130.
- Customer provided VMware Environment.
- Avaya branch gateways including G430 Branch Gateway, and G450 Branch Gateway.

Newer releases of Communication Manager contain the features of the previous releases.

This document is intended for people who perform the product or solution system administration tasks.

Change history

Issue	Date	Summary of changes
14	December 2022	Updated the following sections: • Types of connection to the Avaya S8300E and Avaya common servers • Personal Computer Interface • Wideband Switching video application example • ASAI configuration example
13	June 2022	Updated the following sections to remove the "Internet Explorer" support: • Accessing Communication Manager System Management Interface • Supported browsers
12	July 2021	Removed the following topics as they became obsolete: • Configuring the Directory Application feature • Administering the General Administration section • Administering the LDAP Administration section • Administering the Search Screen settings section • Administering the Detail Screen settings section • Administering the LDAP Filter Settings section • Adding a new external number in the LDAP database • Editing an external number in the LDAP database • Deleting an external number from the LDAP database • Configuring Directory Application
11	June 2021	Updated the “Generating a CSR when third-party signed certificate” section.
10	March 2021	Updated the “Adding an identity certificate for Duplex server” section.
9	February 2021	Updated the references to “Avaya Site Administration” across the document.
8	November 2020	Added the “Administering SIP trunk optimization” chapter.
7	October 2020	In Release 8.1.3, updated the following sections: • Introduction • Purpose • Receiving notification in an emergency • Telephone feature buttons table

Table continues…

Issue	Date	Summary of changes
6	March 2020	In Release 8.1.2, added the following sections: • Configuring log retention period • Data Encryption • Remote key server • Data Encryption password policy • encryptionPassphrase command • Adding encryption passphrase • Changing encryption passphrase • Displaying encryption passphrase and slot assignment • Removing encryption passphrase • encryptionRemoteKey command • Adding remote key server • Removing remote key server • Displaying remote key server and slot assignment • encryptionLocalKey command • Enabling local key store • Disabling local key store • Viewing data encryption status In Release 8.1.2, updated the “Setting up CDR example” section.
5	November 2019	Updated the “Telephone feature buttons table” section.
4	November 2019	Updated the “Changing the Communication Manager IP address” section.
3	August 2019	Updated the “Signing up for PCNs and PSNs” section.
2	July 2019	Updated the “Related Documents for AGL” section.
1	June 2019	Release 8.1

Chapter 2: System Basics

System login

You must log in before you can administer your system. If you are performing remote administration, you must establish a remote administration link. You can also assign the remote administration extension to a hunt group before you log in.

For information about setting up remote administration, do the following:

- Go to the Avaya Support website at http://support.avaya.com.
- See *Administering Avaya Aura® System Manager*.

When you are not using the system, log off for security reasons.

Logging in for remote administration

Procedure

1. To set up remote administration, dial the Uniform Call Distribution (UCD) group extension number.

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

   - If you are on-premises, use an extension number.
   - If you dial a DID number, a dedicated trunk number, or an extension, you get a data tone or a visual confirmation.
   - If you dial LDN, the attendant answers.
   - Request for a transfer to the UCD group extension number. You receive a data tone or visually receive an answer confirmation.
   - Transfer the voice call to your data terminal.

   The system displays a login prompt.

2. Complete the steps for logging into the system.

   For information about setting up remote administration, go to the Avaya Support website at http://support.avaya.com.

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

Out-of-Band management

For information about Out-of-Band management feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Types of connection to the Avaya S8300E and Avaya common servers

The primary support access for system initialization, aftermarket additions, and maintenance are:

- Personal computers
- Service laptops with network PCMCIA cards, and a web browser

The connections to the Avaya S8300E, and Avaya common servers include:

- Direct connection
- Remote connection over the customer LAN

The preferred methods are a direct connection and a remote connection over the customer LAN.

For more information, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Enabling IP forwarding using Services Port VM for AVP Utilities

About this task

IP Forwarding is always disabled after an installation, regardless of the mode of deployment. Use the following procedure to enable IP Forwarding.

Note:

For security reasons, you must always disable IP forwarding after finishing your task.

Procedure

1. Start an SSH session.
2. Log in to AVP Utilities as admin.
3. In the command line, perform one of the following:
   - To enable IP forwarding, type `IP_Forward enable`.
   - To disable IP forwarding, type `IP_Forward disable`.
   - To view the status of IP forwarding, type `IP_Forward status`.

Example

```
IP_Forward enable
Enabling IP Forwarding
Looking for net.ipv4.ip_forward in /etc/sysctl.conf
```

```
Status of IP Forwarding
..Enabled
```

Enhanced Access Security Gateway

Avaya Aura® applications support Enhanced Access Security Gateway (EASG). EASG is a PKI-based challenge-response authentication and authorization solution. Avaya uses EASG to securely access customer systems and provide support and to troubleshoot.

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® remotely and onsite. Access is under the control of the customer and can be enabled or disable at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

Login messages

The system displays either of the two messages during login:

- `Issue of the Day`: Displays warnings to users about unauthorized access. The system displays this message before a successful login.
- `Message of the Day (MOTD)`: Informs authorized users about matters, such as upcoming outages and impending disk full conditions. The system displays this message immediately after a user logs in.

Using the Issue-of-the-Day message

About this task

You can use the Communication Manager file `/etc/issue.avaya` that contains the sample text for the `Issue of the Day` message.

Procedure

1. Log on to the Communication Manager server.
2. On the Command Line Interface (CLI), run the following commands:
   - `cp /etc/issue.avaya /etc/issue`
   - `cp /etc/issue.avaya /etc/issue.net`

Setting Issue-of-the-Day and Message-of-the-Day messages

About this task

Use /bin/vi or /usr/share/emacs to perform the following changes:

Procedure

1. To include the issue PAM module, configure `etc/pam.d/mv-auth`.
2. If you are using telnet to include the text for the `Issue of the Day` message, edit `/etc.issue and /etc.issue.net`.
3. To include the text for the `Message of the Day`, edit `etc/motd`.

   `Message of the Day` is case sensitive. You cannot use the following strings in `Message of the Day`:

   - `[513]` used by FPM, CMSA, VAM
   - `513]` used by connect2
   - `]` used by MSA
   - `Software Version`
   - `Login:`
   - `Password:`
   - `Challenge:`
   - `ogin`
   - `ogin:`
   - `incorrect logoin`
   - `assword`
   - `hallenge`
   - `SAT`
   - `SAT` cannot be executed on a standby server

   When searching for the strings, white space and case are ignored.

   For more information on setting login messages and interaction with individual access services, see the *Communication Manager Administrator Logins* white paper.

Log off the system

For security reasons, log off every time you leave your terminal. If you use terminal emulation software to administer Communication Manager, log off the system and quit the emulation program before switching to another software package.

Logging off the system

Before you begin

The system does not log off if any of the features or alarms are active. Disable any features or alarms that are active before you log off the system.

Procedure

1. On the command line interface, type `Logoff`.
2. Press **Enter**.
3. At the **Proceed with Logoff** prompt, type y.

   If you log off with the alarm origination disabled, Avaya support services do not receive alarm notifications when the system generates an alarm. For more information about alarms, see the maintenance book of your system.

User profiles and logins

Using Authentication, Authorization, and Accounting (AAA) services, you can store and maintain administrator account information on a central server. Login authentication and access authorization are administered on the central server.

For information about administering user profiles and logins in AAA services, see *Avaya Aura® Communication Manager Feature Description and Implementation*, and *Maintenance Commands for Avaya Aura®, Branch Gateways and Servers*.

Establish daylight-saving rules

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

You can set up 15 customized rules for daylight-saving time. With this setting, Communication Manager administrators with servers in different time zones can set up a rule for each server. A daylight-saving time rule specifies the exact time when you want to transition to and from daylight-saving time. The rule also specifies the increment at which to transition, for example, 1 hour.

To establish Daylight Saving Time (DST) rules

Procedure

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

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

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

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

   Note:

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

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

   Note:

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

Displaying daylight saving time rules

Procedure

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

   The system displays the Daylight Saving Rules screen. Verify the information you entered is correct.

Set Time of Day Clock Synchronization

Using Time of Day Clock Synchronization, you can enable a server to synchronize its internal clock with the 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.

Administering Clock Synchronization over IP

About this task

You can use Clock Synchronization over IP (CSoIP) feature on G450 Branch Gatewayand G430 Branch Gateway to provide system clocks across IP networks.

Procedure

1. Configuring the synchronization reference for the gateway on page 30
2. **(Optional)** Configuring the synchronization reference for the BRI trunk board on page 31.
3. Setting the synchronization on page 31
4. Enabling the synchronization on page 31
5. Configuring the IP synchronization on page 31
6. Configuring the IP synchronization for the gateway on page 32
7. Configuring the IP synchronization for the network region on page 32

Configuring the synchronization reference for the gateway

Procedure

1. Type `list synchronization media-gateway` to determine if any gateway is set up for synchronization.
2. Type `change synchronization media-gateway n`, where *n* is the number of the gateway that requires synchronization.
3. In the **Primary** field, type the location of T1 media module. Obtain this location from the media modules available for the Synchronization list. Ensure that you choose a working synchronization source.
4. (Optional) In the **Secondary** field, type the location of T2 media module.
5. Select **Enter** to save the changes.

Configuring the synchronization reference for the BRI trunk board

About this task

Use this procedure only for the configurations that use BRI trunks.

Procedure

1. Type `change bri-trunk-board n`, where *n* is the board location that you want to set up as a synchronization source.
2. Set the **Synch Source** field to `y`.
3. Select **Enter** to save the changes.

Setting the synchronization

About this task

Use this procedure to set a synchronization-capable circuit pack as the reference source for system synchronization signals. Synchronization-capable circuit packs include:

- DS1 trunks
- BRI trunks
- IP Server Interfaces (IPSIs)
- Circuit Emulation Services (CES)
- Tone-Clocks

Procedure

Type `set synchronization n`, where *n* is the Tone-Clock location or the synchronization source location.

Enabling the synchronization

About this task

Use this procedure only if you have previously turned off the synchronization by `disable synchronization`. Use this procedure to return the control of selection of the synchronization source to the Synchronization Maintenance subsystem.

Procedure

Type `enable synchronization media-gateway n`, where *n* is the number of the gateway.

Configuring the IP synchronization

Procedure

1. Type `change system-parameters features`.
2. Click **Next** until you see the **IP Parameters** section.
3. Set the **Synchronization over IP** field to `y`.

4. Save the changes.

Configuring the IP synchronization for the gateway

Procedure

1. Type `change media-gateway n`, where *n* is the number of the gateway for which you want to enable IP synchronization.
2. Set the **Use for IP Sync** field to y. If you do not want to configure the gateway to synchronize with other gateways in the network, set the field to n.
3. Select **Enter** to save the changes.

Configuring the IP synchronization for the network region

Procedure

1. Type `change ip-network-region n`, where *n* is the network region number in which you want to enable IP synchronization.
2. Click **Next** until you see the Inter Network Region Connection Management screen.
3. Set the **Sync** field to y. If you do not want to configure the region to synchronize with other network regions, set the field to n.
4. Save the changes.

Disabling synchronization

About this task

Use this procedure to prevent switching between clock sources.

Procedure

Type `disable synchronization media-gateway n`, where *n* is the number of the gateway.

Setting up the network time protocol

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **NTP Configuration**.

   The system displays the Network Time Protocol (NTP) Configuration page.

4. Enable or disable the NTP mode.
5. In NTP Servers, type the primary server, secondary server (Optional), and tertiary server (Optional) details.
6. Click **Apply**.

Using the bulletin board

Use Communication Manager 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. The system does not display this notification 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, the system displays a message at login indicating how much of its capacity is currently used (for example, 84%). If the bulletin board reaches maximum capacity, new messages overwrite the oldest messages.

Note:

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

Displaying messages

Procedure

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

   The system displays the Bulletin Board screen.

Posting a message

About this task

Post a message to the bulletin board. The message can be about a problem related to a new trunk group. A representative from Avaya will reply to your message.

Procedure

1. Type `change bulletin-board`.

2. Press `Enter`.

   The Bulletin Board screen displays.

   The message space within the bulletin board contains three pages. The first page has 19 lines, however 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 these are noted with an asterisk (*). The second and third pages each have 20 lines, and you can enter text on any of these lines. The system automatically enters the date the message was posted or last changed to the right of each message line.

3. Type your message.

   You can enter up to 40 characters of text for each 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 1 of any page. You cannot indent text on the bulletin board. The **Tab** key moves the cursor to the next line.

4. Save the changes.

Deleting messages

Procedure

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

   The system displays the Bulletin Board screen.

3. Enter a space as the first character on each line of the message you want to delete.
4. Press `Enter`.
5. Save the changes.

Save translations

Use `save translation` to commit the active server translations (volatile) in memory to a file (non-volatile). The translation will either complete or fail. For Linux platforms, a filesync process copies the translation file to the standby server.

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

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

The `save translation` command does not run and the system displays an error message in the following cases:

- An administration command changes the translation data.
- The Communication Manager Web interface Pre-Upgrade Step locks the translations.

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

For information on the `save translation` command and the command syntax descriptions, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Performing backups

For information on performing backups to your system, see *Maintenance Procedures forMaintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Changing the Communication Manager IP Address

About this task

If you want to shift the Communication Manager from one network location to another network location, then you must change the IP address of the Communication Manager. After changing the IP address on Communication Manager, you must change the IP address of the Communication Manager virtual machine in the vCenter **vApp options** section.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Network Configuration**.

   The Network Configuration page appears.
4. In the **IP Configuration** field, type the IP address of the new network location.
5. Click **Restart CM**.

   System displays a message confirming to restart. You must restart the server for the changes to take effect.
6. Click **Restart Now** or **Restart Later**.

Chapter 3: System Planning

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

System configuration

Planning Your System

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 check 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. 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:

1. Type `list configuration port-network`.
2. Press `Enter`.

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

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

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

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

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

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

Viewing a list of port boards

Procedure

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

   The System Configuration screen shows all the boards on your system that are available for connecting telephones, trunks, data modules, and other equipment. You can see the board number, board type, circuit-pack type, and status of each port on the board. 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.

Understanding equipment addressing

Where addressing is used

You must enter a port or a slot in many sections in the administration interface. The port or slot is an address that describes the physical location of the equipment you are using.

Address format

A port address consists of four parts:

- Cabinet: The main housing for all the server equipment. Cabinets are numbered starting with 01.
- Carrier: The rack within the cabinet that holds a row of circuit packs. Each carrier within a cabinet has a letter: A to E.
- Slot: The space in the carrier that holds an individual circuit pack. Slots are numbered 01-16.
- Port: The wire that is connected to an individual piece of equipment (such as a telephone or data module). The number of ports on a circuit pack varies depending on the type.

Example

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

Communication Manager server separation

In earlier releases, Communication Manager duplex configurations required a cable for connecting two Communication Manager instances with dedicated Communication Manager server hardware. Starting from Communication Manager Release 7.1 and later, you can physically separate the Communication Manager duplex instances.

For server separation support, the duplex servers must be in the same availability zone (AZ) to ensure that both the servers are in the same subnet. Availability zone also allows high-availability (HA) protecting the application from datacenter failures.

Following are the minimum requirements for software duplex connectivity that must be met between the two Communication Manager instances:

- Total capacity must be 1 Gbps or more.
- Round-trip packet loss must be 0.1% or less.
- Round trip delay must be 60 ms when Application Enablement Services is not configured and 30 ms when Application Enablement Services is configured.
- The duplication ports of both servers must be on the same LAN/IP subnet.
- Duplication link encryption must be disabled for the busy-hour call rates that results in greater than 40% CPU occupancy.
- CPU occupancy on the active server must be less than 65% to allow memory refresh from the active to standby server.

Dial plan

Dial Plan

The system interprets dialed digits based on the dial plan. If you dial 9 on your system to access an outside line, the system finds an external trunk for that number because the dial plan is set that way.

The dial plan also defines the number of digits that indicate certain types of calls. For example, the dial plan might indicate that all internal extensions are four-digit numbers that start with either 1 or 2. An example will illustrate how to read the dial plan of your system.

Note:

In Communication Manager 8.0 the maximum length of a displayed extension (including punctuation) is 16 characters.

Dial plan access table

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

Dial plan parameters table

The Dial Plan Analysis table and the Dial Plan Parameters table define your dial plan. You can set system-wide parameters for your dial plan, or define a Dial Plan Parameters table according to each location.

Uniform dial plan

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

Displaying your dial plan

Procedure

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

Modifying your dial plan

Procedure

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

Adding extension ranges

About this task

As your requirements increase, you might 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.

As an example, add a new set of extensions that start with 3 each and are four-digit long (3000 to 3999).

Procedure

1. Go to the administration interface.

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

Multi-location dial plan

A customer migrates from a multiple independent node network to a single distributed server. The gateways of the single distributed server are distributed across a data network. It may 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. The extensions and attendants were provided in a multiple independent node network. However, they appear to be unavailable when customers migrate to a single distributed server.

Example

In a multi-location department store, each location has its own switch in a multiple independent node network. The same extension is used to represent a specific department across all stores. For example, extension 123 is assigned to the luggage department in all stores. If the customer migrates to a single distributed server, a user can no longer dial 123 to reach the luggage department in the store of their preferred location. To do this, the user must dial the complete extension to connect to the proper department.

In a similar scenario, using the multi-location dial plan feature, a user can dial a shorter version of the extension in place of the complete extension. For example, a customer can continue to dial 123 instead of 222-123.

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

Note:

To administer the multi-location dial plan feature, set the **Multiple Locations** field to `y` on the System Parameters Customer Options (Optional Features) screen. To check if this is enabled, use the `display system-parameters customer-options` command.

Location numbers

The equipment gets location numbers as follows:

- IP telephones obtain their location numbers indirectly. A location number is administered on the IP Network Region screen that applies to all the telephones in that IP region.
- Non-IP telephones and trunks inherit the location numbers of the hardware they are connected to, such as the cabinet, remote office, or gateway.

- IP trunks obtain their location from the location of the associated signaling group. Direct administration, which is only possible for signaling groups for remote offices or the methods described for IP telephones above determine the location.

Location administration

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

For information on how to administer the location per station, see the Administer location per station on page 140 section.

For information on the description of the **Location** field on the Stations with Off-PBX Telephone Integration screen, see the *Avaya Aura® Communication Manager Screen Reference*.

Prepending the location prefix to dialed numbers

About this task

To assign the location prefix from the caller's location on the Locations screen, complete the following steps:

Procedure

1. Go to the administration interface.
2. Enter `change uniform-dialplan`.
3. In the **Insert Digits** field, enter digits between 0-9 or enter an Ln string, where n is a digit between 1-11. The Ln entry accepts only the first n digits from the **Prefix** assigned to the calling party's location on the Locations screen. The Ln entry is used for short-to-long mapping. For example, the Ln entry is used to convert a short number, such as 83529 to a long number, such as 1303-538-3529. However if you have more than one prefix assigned per location, use the Calltype Analysis screen.

   Note:

   If you are entering an Ln string, ensure that the **Multiple Locations** field is enabled on the system-parameters customer-options screen.
4. Press `Enter` to save your changes.

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

Other options for the dial plan

You can set up different options by using the dial plan. For example, you can establish a dial plan to enable users to dial only a single digit to reach another extension. Using another dial plan, users can dial two digits to reach one extension, and three digits to reach another. This is

particularly useful in the hospitality industry, where users can simply dial a room number to reach another guest.

If you have Communication Manager 5.0 or later, you can administer dial plans for each 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 Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Feature access codes

Users can use Feature Access Codes (FAC) 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 the FAC for the Last Number Dialed is *33, then users can re-dial a telephone number by entering the FAC, rather than requiring a Last Number Dialed button. Many features already have factory-set feature access codes. You can use these default codes, or you can change them to codes that make more sense to you. However every FAC must conform to your dial plan and must be unique.

Adding feature access codes

About this task

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

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

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

Procedure

1. Go to the administration interface.
2. Enter `change dialplan analysis` or `change dialplan analysis location n`, where n represents the number of a specific location. Press `Enter`.

   The system displays the Dial Plan Analysis screen.
3. On the Dial Plan Analysis screen, move the cursor to an empty row.
4. Type `3` in the **Dialed String** column, and then tab to the next field.
5. Type `2` in the **Total Length** column, and then tab to the next field.
6. Type `FAC` in the **Call Type** column.
7. Press `Enter` to save your changes.

Changing feature access codes

About this task

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

Tip:

To remove an FAC, delete the existing FAC and leave the field blank.

For example, to change the FAC for Call Park to *72, perform the following procedure:

Procedure

1. Go to the administration interface.
2. Enter **`change feature-access-codes`**.
3. Press `Enter`

   The system displays the Feature Access Code (FAC) screen.
4. On the Feature Access Code (FAC) screen, type the new code *72 over the old field in the **Call Park Access Code** field.
5. Press `Enter` to save your changes.

Administering Dial Plan Transparency

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

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

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

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

Control the features your users can access

Class of service and class of restriction give you great flexibility with what you allow users to do. If you are in doubt about the potential security risks associated with a particular permission, visit the Avaya Support website at http://support.avaya.com.

Features and functions

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

Class of service

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

Class of restriction

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

Enabling system wide settings

About this task

There are some settings that you enable or disable for the entire system, and these settings affect every user. You can check the various System Parameters screens and decide which settings best meet the needs of your users.

Procedure

1. 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 on your own.

2. Type `change system-parameters`.
3. Press **Help** to see which types of parameters you can change.

In some cases, an Avaya technical support representative is the only person who can make changes, such as to the System-Parameters Customer-Options screen.

4. In the system, type list usage to see all the instances of an object, such as an extension or IP address.

   This is useful when you attempt to change administration and receive an in use error.

   For more information, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Changing system parameters

About this task

You can modify the system parameters that are associated with some of the system features. For example, you can use the system parameters to play music if callers are on hold or to provide 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 organizational needs.

As an example, to change the number of rings between each point for new coverage paths from 4 to 2 rings, complete the following steps:

Procedure

1. Go to the administration interface.
2. Enter `change system-parameters coverage/forwarding`.
3. Press `Enter`.

   The system displays the System Parameters Call Coverage/Call Forwarding screen.
4. In the **Local Coverage Subsequent Redirection/CFWD No Answer Interval** field, type `2`.
5. Press `Enter` to save your changes.

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

WAN Bandwidth Limits between Network Regions

Bandwidth limits

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

Bandwidth limits can be administered in terms of:

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

Considerations for WAN bandwidth administration

Collect design information

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

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

Typical bandwidth usage

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

Packet Size	10 ms	20 ms	30 ms	40 ms	50 ms	20 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
G.722.2	NA	43	NA	34	NA	31

These values are not significantly different from the actual bandwidth used for 8–byte L2 WAN headers and 10–byte L2 WAN headers. In some cases, the rounded up values shown above are greater than the values used for 10 bytes.

The bandwidth usage numbers shown above have 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 is modeled by administering the CAC-BL limits in terms of number of connections rather than bandwidth used.

Setting bandwidth limits between directly connected network regions

Procedure

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

Administering Denied or Invalid Calls

About this task

You can administer your system to reroute denied or invalid calls to an announcement, the attendant, or to the vector directory number.

The following calls are rerouted.

- All outward restricted call attempts to routed to an announcement at extension 2040.
- All incoming calls that are denied to routed to the attendant.
- All invalid dialed numbers are routed to an announcement at extension 2045.
- All invalid incoming calls are routed to a vdn at 2050.

The steps for the rerouting are as follows:

Procedure

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

   The system displays the Feature-Related System Parameters screen.
2. In the **Controlled Outward Restriction Intercept Treatment** field, type `announcement`.

   The system displays a blank field.
3. In the 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`.

   The attendant uses this to handle incoming calls that have been denied.
5. In the **Invalid Number Dialed Intercept** field, type `announcement`.

   The system displays a blank field.
6. In the blank field, type `2045`.

   This is the extension of an announcement you recorded earlier.
7. In the **DID/Tie/ISDN Intercept Treatment** field on Page 1, type `vdn`.

   The system displays a blank field.
8. In the blank field, type `2050`.

   This routes all incoming invalid calls to the specified vector directory number.

   For more information on how to create VDN, see Adding a Vector Directory Number.
9. Save the changes.

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. Avaya Aura® Media Server is used as a repository for announcements and music sources for the Music-on-hold feature.

For more information on locally sourced Music-on-Hold, see *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. Use this feature to provide 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 gateway. The VAL or vVAL boards are assigned to an audio group. The audio group is then assigned to an announcement or audio extension as a group sourced location. When an incoming call requires an announcement or Music-on-Hold, the audio source that is closest to the incoming call trunk plays.

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

Audio groups

An audio group is a collection of identical announcements 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.

With centralized SIP trunking, the chances of having the closest audio source to the caller at the main or survivable core data centers are high. For playback to occur in survivable mode, remote gateways must be configured with the announcement and music files. So, it is recommended that Audio Groups are configured to ensure the solution is capable of playing announcements and music, regardless of the survivability status of the system.

For example: if a solution consists of a main data center with media server, survivable core data center with media server and survivable remote with gateway, then an audio group containing the three audio source locations of a media server from each data center and the remote gateway should be constructed. This ensures playback capability regardless of whether the solution is in normal or rainy day mode.

Music-on-hold groups

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

Music-on-hold sources

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

Adding an audio group

Procedure

1. Enter **add audio-group n**, where n is the group number you want to assign to this audio group. To assign the next available audio group number in the system, enter add **audio-group n** next.

   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, vVAL location designators, or the media server for each audio source in the audio group.
4. Press `Enter` to save your changes.

Adding a Music-on-Hold group

Procedure

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

   The system displays the MOH Group screen.

2. In the **Group Name** field, type in an identifier name for the Music-on-Hold group.
3. In the **MOH Source Location numbered** fields, type in the Music-on-Hold VAL or vVAL source locations.
4. Press `Enter` to save your changes.

Setting music-on-hold system parameters

About this task

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

Note:

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

Procedure

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

   The 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 use for MOH: an extension (ext), an audio group (group), or a port on a circuit pack (port).
4. In the text field that the system displays to the right of your **Type** selection, type the extension number, the audio group, or the port address of the music source.
5. In the **Music (or Silence) on Transferred Trunk Calls** field, type `all`.
6. Press `Enter` to save your changes.
7. Now administer a class of restriction with **Hear System Music on Hold** set to y for local users to hear Music-on-Hold.

Providing music-on-hold service for multiple tenants

Before you begin

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

About this task

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

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

Procedure

1. Enter **`change music-sources`** on the administration interface.
2. For Source No 1, enter `music` in the **Type** column.

   The system displays a **Type** field under the **Source** column.
3. In the **Type** field, enter `port`.

   The system displays a blank text field.
4. Enter the port number, `01A1001` in this case, in the text field.
5. In the **description** field, enter `Country`.
6. Move to Source 3, and enter music in the *Type* column, `port` in the **Type** field, `01A1003` for the port number, and `Classical` for the **Description**.
7. Press `Enter` to save your changes.
8. Enter **`change tenant 1`**.

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

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

    Note:

    The attendant group number must also appear in the **Group** field of the Attendant Console screen for this tenant.
11. In the **Music Source** field, type `1`.

    Callers to this tenant hear country music while on hold.
12. Press `Enter` to save your changes.
13. To administer the next partition, enter **`change tenant 2`**.
14. Administer this tenant, Insurance Agent, to use Attendant Group 2 and Music Source 3. Be sure to change the Attendant Console screen so that this attendant is in group 2. The callers of this tenant hear classical music on hold.

Receiving Notification in an Emergency

If one of your user calls an emergency service, someone for e.g. the front desk or receptionist of the building should get the caller information. So when the emergency personnel arrives,

receptionist can use the caller information and identify the user. 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 receptionist's telephone shows the name and the number of the person who placed the emergency call. The telephone also ring with a siren-type alarm, which receptionist must acknowledge to cancel.

Note:

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

Ensure that the extensions you notify belong to physical digital-display telephones. 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.

Refer to *Telephone Reference* for a list of telephone types.

About this task

The following example illustrates how to set up the system to notify the attendant and the security guards at all 3 entrances when someone dials the emergency number 5555. All three guards must acknowledge the alert before it is silent.

Procedure

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

   5555 is the number in our example 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, use route pattern 1 for local calls.
5. In the **Call Type** field, type `alrt`.

   The system 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.

Finally, ensure that all security personnel and the attendant must 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. In the **SNMP Inform to Notify Adjunct When DCP and H.323 Stations Go In-Service** field, do the following:

    - If you have DCP or H.323 phones and Emergency Location Management Solution, type `y`.
    - If you do not have DCP or H.323 phones, or Emergency Location Management Solution, leave this field as `n`.

    When a DCP station comes into service, or a H.323 station registers, the Communication Manager sends SNMP messages to a trap receiver.

14. **(Optional)** In the **SNMP Inform to Notify Adjunct When SIP Station Dials Emergency Call** field, do the following:

    - If you have configured Emergency Location Management Solution as an ELIN server with Session Manager, leave this field as `n`.
    - If you have Emergency Location Management Solution, but have not configured it as an ELIN server, type `y`.

    For more information on administering the ELIN server, see *Administering Avaya Aura® Session Manager*.

    When a SIP station places an emergency call, the Communication Manager sends SNMP messages to a trap receiver.

15. Press `Enter` to save your changes.

Notifying a digital pager of an Emergency

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

Before you begin

- Administer a **crss-alert** button on one of the following:
  - For Attendant Console, use the **`change attendant`** command
  - For Digital telephone set, use the **`change station`** command
- In the **ARS Digit Analysis** Table, set the emergency numbers in the **Call Type** column to **alrt** (crisis alert).

- You need a digital numeric pager.

Procedure

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

   The system displays the Crisis Alert System Parameters screen.

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

   With this setting, you can use the Crisis Alert to a Digital Pager feature and causes an additional crisis alert administration fields to appear.

4. In the **Originating Extension** field, type a valid, unused extension to send the crisis alert message. As an example, type `7768`.
5. In the **Crisis Alert Code** field, type `911`.

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

6. 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.

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

   This is the length of time between retries.

8. In the **Main Number** field, type the number to display at the end of the pager message, such as `303-555-0800`.
9. In the **Pager Number** field, type the number for the pager, such as `303-555-9001`.
10. In the **Pin Number** field, type `pp77614567890`.

    This is the PIN, 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.

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

    This is the duration the DTMF tone is heard for each digit.

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

    This is the duration between DTMF tones for each digit.

13. Save the changes.

    For more information about Crisis Alert feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Other useful settings

Many settings control how your system operates and how your users telephones work. You can administer most of these settings through one of the System Parameters screens. This section describes a few items you can enable in your system to help your users work more efficiently. For a more detailed description of the available settings, see Feature-Related System Parameters.

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 about the Automatic Callback feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Automatic hold

You can set a system-wide parameter for 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 enable this feature, the active call drops when the user presses the second line button.

Bridging to a call that has gone to coverage

You can allow users to bridge to a call that rings at their extension and then goes to coverage before they answer. For more information about Temporary Bridged Appearance feature, see *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 about the Distinctive Ringing feature, see *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.

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. For more information about Distinctive Ringing, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Controlling users calls

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 can 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 affect the required 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 requires the additional step of explaining where you want 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. For more information, 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

About this task

You can allow specific users to change their CORs from their telephones by 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. Use the Station Lock feature to change their own COR.

Before you begin

- Ensure that **Change COR by FAC** field is set to `y` on the System-Parameters Customer-Options (Optional Features) screen.

  Note:

  You cannot enable both **Change COR by FAC** and **Tenant Partitioning**.

- Ensure that each user (who you want to allow to change a COR has a class of service with console permissions).

About this task

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

Procedure

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. To save your changes, press `Enter`.

   To define the password.
5. Type `change system-parameters features`. Press `Enter`.

   The system displays the Feature-Related System Parameters screen.
6. To find the Automatic Exclusion Parameters section, press `Next Page`.
7. Move to the **Password to Change COR by FAC** field, and type `12344321`.

   This field determines whether or not Communication Manager requires the user to enter a password when they try to change their COR. You must have a password.
8. To save your changes, press `Enter`.

Station Lock

Use the Station Lock feature to lock a telephone to prevent others from making outgoing calls from the telephone. You can activate the Station Lock feature by using a button or feature access code. You can lock and unlock the telephones remotely.

Using Station Lock, users can:

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

Station Lock is activated by pressing a telephone button, which lights the button indicator, or by dialing a Feature Access Code (FAC).

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

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

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

You can lock or unlock a station from any other station if the FAC is used and the Station Security Code is known. You cannot lock the attendant console but you can use it to lock or unlock other stations. You can lock or unlock a station using a remote access trunk.

For more information about Station Lock, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Station Lock by time of day

With Communication Manager 4.0 and later, you can lock stations using a Time of Day (TOD) schedule.

To engage the TOD station lock or unlock, you do not have to dial the station lock or unlock FAC.

When the TOD feature activates the automatic station lock, the station uses the COR assigned to the station lock feature for call processing. The COR used is the same for manual station locks.

The TOD lock or 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 and the station invokes a transaction which is denied by the Station Lock COR, the system displays Time of Day Station Locked. Whenever the station is within a TOD Lock interval and the special dial tone is administered, the user hears a special dial tone instead of the normal dial tone.
- 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 the special dial tone when the station is off hook.

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

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

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

The TOD feature does not unlock a manually locked station.

Note:

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

Chapter 4: Administer Communication Manager on Avaya servers

The chapter describes how to administer Communication Manager on the supported Avaya servers after the product is installed and tested.

The target audience includes system administrators and users with data-networking experience in data products and technology, and knowledge of the call processing engine of Communication Manager. In a converged network, voice and data are both sent over a corporate local area network (LAN). Such a configuration can provide primary or standby telephony, and communication-processing capabilities.

For more information, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Overview about administering Avaya servers

Administer the following to set up and maintain your Avaya server with a branch gateway:

- The branch gateway and its internal processors, typically using a command-line interface (CLI).
- S8300E or an Avaya common server using the server web interface.
- Call processing features using Communication Manager.

For more information about Avaya servers, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Survivable remote servers configuration

An S8300E or an Avaya common server can either be configured as a primary call-processing controller or as a survivable remote server, which is also called a Local Survivable Processor (LSP). The survivable remote server can take over call processing if the primary call-processing system, such as another Avaya server, is unavailable for any reason. Such reasons include network failure or server problems. The S8300E or Avaya common server can either be the primary or the survivable remote server. This server is set up to operate as a primary or a

standby survivable remote server during the configuration process using a web server interface. The license file determines the mode in which the server operates, and the Configure Server web page provides supplementary instruction.

If the S8300E or Avaya common server loses contact with its gateway, the gateway retains its last status until Link Loss Delay Timer (LLDT) expires. The default for LLDT is five minutes, however, this interval is administrable using the **Link Loss Delay Timer (minutes)** field on the IP-Options System Parameters screen. After LLDT expires, the system removes all boards and deletes all the call-processing information. However, if the gateway loses contact with the S8300E or Avaya common server, the gateway tries to reconnect for a period of one minute. If reconnection fails, the gateway then tries to connect with another server in its controller list. If the primary server is a survivable remote server, it starts looking at the top of its MGC list to reconnect to the primary server. Otherwise, it starts down the list of alternative servers. When a functional S8300E or Avaya common server is located, the gateway indicates the server of its current call state, and the server maintains the connections until the users disconnect.

If the primary call-processing server goes offline and a survivable remote server is available as a standby unit, call processing happens as follows:

- IP telephones and gateways that were previously using the primary server try to register with the standby server for call processing, provided that they have been administered to do so in the controller list by using the **`set mgc list`** command.
- The standby server, which is the survivable remote server, goes into license error mode, and then starts call processing. The standby server 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, however, no features are supported on the call.

  Note:

  The license error mode runs for up to 30 days, and if the problem is unresolved, the system goes into No License Mode and administration and some commands are restricted.

- If the standby server is rebooted, all devices return to using the primary server for call-processing service. Any calls in progress on the standby survivable remote server are dropped when the reboot occurs as the change back to the primary server is not call preserving.

The survivable remote server provides full functionality and feature.

For more information about Avaya servers, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Command line interface administration

Instead of using Device Manager, you can access the server command line interface (CLI) using Telnet and an IP address.

For more information about SNMP alarms, see *Avaya Aura® Communication Manager SNMP Administration and Reference*.

S8300E and Avaya common server administration

You can install a Communication Manager OVA on an S8300E or Avaya common server to control its operation over the corporate network. The server performs the following functions:

- Backing up and restoring call processing, server, and security data using System Management Interface (SMI)
- Checking server and process status
- Monitoring the status of the system
- Updating and managing patches
- Installing license file
- Managing the security configuration for the server
- Installing new software and reconfiguring the server as required
- Performing system and alarm configuration
- Rebooting or shutting down the server
- Managing users and passwords

For more information about Avaya servers, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Access and administer Communication Manager

You can access and administer Communication Manager by:

- Starting a SAT session
- Accessing SMI

Enabling or disabling Telnet service for Communication Manager

Procedure

1. Log in to Communication Manager System Management Interface.
2. Click **Administration** > **Sever (Maintenance)**.
3. On the left hand navigational panel, click **Security** > **Server Access**.

4. On the Server Access page, in the **SAT over Telnet (5023)** field, do one of the following:
   - Select **Enable** to enable **SAT over Telnet (5023)**.
   - Select **Disable** to disable **SAT over Telnet (5023)**.
5. Click **Submit**.

Starting a SAT session

Before you begin

- Before you use Telnet, you must enable the Telnet service for Communication Manager.

Procedure

1. Open a secure session using PuTTY or Telnet.
2. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
3. Log on to the server using an appropriate user ID.
4. Suppress alarm origination.
5. Press `Enter`.

Access System Management Interface

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Mozilla Firefox Release 93
- Google Chrome Release 91
- Microsoft Edge Release 93

Note:

- From Avaya Aura® Release 8.1.3.5 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

Accessing Communication Manager System Management Interface

About this task

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

Note:

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

Procedure

1. Open a compatible web browser.
2. In your browser, choose one of the following options based on the server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the specific server, or any other Avaya common server in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8300E or Avaya common servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Enhanced Access Security Gateway (EASG), you must have an EASG tool to generate a response for the challenge that the Logon page generates.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Accessing Server Administration Interface

About this task

Using SMI, you can configure, maintain, and troubleshoot the Communication Manager server.

Procedure

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

A list of links on the left side of the screen lists the tasks that you can perform through SMI.

For help with any of these tasks, click **Help** on the home page.

Server Administration Interface tasks

Key tasks that administrators typically perform on the Communication Manager Servers are summarized in this section. For more detailed information, see online help.

File copy to the server

You must copy files to an S8300E or Avaya common server from another computer or server in the network, or upload from a directly connected laptop computer. The types of files copied to the server include license files, system announcements, and files for software upgrades.

Download files to the server from the web link to copy files to the server from another server on the network. It works like the Upload Files screen.

Error resistant download through https

Communication Manager provides a more robust system upgrade experience.

After a Communication Manager upgrades, the system:

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

SNMP setup

You can set up Simple Network Management Protocol (SNMP) services on the server to provide a means for a corporate NMS to monitor the server and send alarm notifications to a services

agency, to a corporate NMS, or both. For more information about administering SNMP, see *Avaya Aura® Communication Manager SNMP Administration and Reference* guide.

To activate SNMP alarm notifications for devices, use the SNMP Traps screen and set up SNMP destinations in the corporate NMS. SNMP traps for other devices on the network can be administered using Device Manager. For more information about administering SNMP, see *Avaya Aura® Communication Manager SNMP Administration and Reference*.

Note:

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

Main and survivable server Split Registration Prevention feature administration

Split registration prevention

Split registrations occur when resources in one network region are registered with different servers. Split registrations occur when a system malfunction activates survivable servers, telephones register with the main server, and gateways register with the survivable server. The survivable server is either a survivable remote server (SRS) or a survivable core server (SCS). The telephones registered with the main server are isolated from the trunk and VoIP resources.

With the split registration prevention feature, an administrator can administer telephones and gateways to register either with the main server or the survivable server.

The main server ensures that all the gateways and telephones in a network region register with the same server. The gateways and telephones can register either with the survivable server or with the main server after the main server is restored. Administrators can configure telephones and gateways to register with active survivable servers. The split registration prevention feature keeps branch-oriented operations intact with local trunk and VoIP resources.

Activating Split Registration Prevention

Procedure

1. Log in to the Communication Manager System Administration Terminal (SAT) interface.
2. At the command prompt, type `change system-parameters ip-options`.
3. Go to Page 2.

4. Set the value of the **Force Phones and Gateways to Active Survivable Servers?** field to `y`.

Sequence of events for split registration prevention

If you are an administrator, you can enable the Split Registration Prevention feature. If the main server is reset or the network splits, causing a gateway to deregister, the following sequence of events occurs:

1. The gateway registers with the survivable server.
2. The survivable server reports its active status to the main server.
3. The main server deregisters all gateways and telephones in the regions backed up by the survivable server.
4. The main server enables the endpoints in those regions to reregister when the day and time specified in the time-day window is reached or until the **`enable mg-return`** command is run.

Alternate ways to manage split registration between the main and survivable servers

- On the **System Parameters Media Gateway Automatic Recovery Rule** screen, set the **Migrate H.248 MG to primary:** field to `immediately`. When you administer this option, the media gateway registers with the main server to test the network stability.

  For more information on recovery rules, see Recovery to the main server on page 68.
- Use the Split Registration Prevention feature described in this section.

If you prefer aggregation at the survivable server, the main server or the survivable server disables the network regions associated with the survivable server. This causes all the telephones and gateways in the regions to register with the survivable server. The telephones and gateways cannot reregister to the main server or the survivable server till one of the following conditions is satisfied:

- At least one gateway reaches the time configured in **time-day-window**.
- The administrator runs the **`mg-return`** command.
- Re-registration to the main server or the survivable server ends in the following situations:
  - The survivable server becomes inactive.
  - One hour elapses after the administrator runs the **`enable-mg return`** command.
  - The administrator runs the **`disable mg-return`** command.
- The survivable server deregisters from the main server or the survivable server.

Recovery to the main server

The allowable recovery rules are:

- `none`
- `immediate`
- `time-day-window`

Important:

You must administer the same recovery rule for gateways with the same survivable server.

The way the **immediate** rule operates depends on the type of server the gateways are registered to. If the following conditions are met, the gateways can reregister to the main server after the network stability period expires:

- The survivable server is Survivable Core Server (SCS).
- There are gateways registered with the main server.

The default duration of the network stability period is three minutes. You can change the duration on the mg-recovery-rule screen. If all the gateways are on SCS, then the network regions assigned to the survivable server are disabled. If the survivable server is Survivable Remote Server (SRS), then the network regions are disabled even if there are some telephones and gateways registered with the main server.

If you administer the **time-day-window** (TDW) rule, all the associated network regions are disabled regardless of the type of the survivable server. When the TDW day and hour is reached, the system activates the NRs, and all the gateways and telephones in those NRs return to the main server. At the end of the hour, the system checks whether all the gateways have returned. If the gateways have returned to the main server, the system reactivates the feature for the next event. If not, the NRs are disabled, causing all the gateways to register with the survivable server.

With the **`enable mg-return`** command, you can re-register gateways to the server. If some gateways remain unregistered from the main server in the active state and the survivable server in the active state, the system again disables the network regions. If the survivable server deregisters from the main server, the main server does not receive information about the status of the survivable server. If the main server does not receive information about the status of the survivable server, the main server activates all the network regions associated with the survivable server.

Note:

If there are port networks on SCS, it will remain active even if all the gateways reregister to the main server. You can use the `get forced-takeover ipserver-interface` command to force registration to the main server.

Telephones in a network region automatically deregister when all the gateways and port networks deregister from the survivable server.

Network region state

Network region state

Use the **status nr-registration** command to view information about the status of the network regions and the link status of the media gateways in the network regions. Use the **enable nr-registrations nnn** command to activate network regions, where nnn is the network region number. Use the **disable nr-registrations nnn** command to disable a network region.

The Split Registration Prevention feature automatically deactivates network regions that the survivable server controls.

To activate or deactivate network regions, on the system-parameters ip-options screen, set the **Force Phones and Gateways to Survivable Servers** field to `n`.

Viewing network region status

Procedure

1. Log in to the Communication Manager System Administration Terminal (SAT) interface.
2. At the command prompt, type `status nr-registration all-regions`.
3. Press `Enter`.

   For more information on the **status nr-registration network-region x command**, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Viewing the gateway link status in a network region

Procedure

1. Type `status nr-registration network-region x`, where x is the name or number of the network region.
2. Press `Enter`.

   For more information on the **status nr-registration network-region x** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Viewing the gateway link status in all regions

Procedure

1. Type `status nr-registration survivable-processor node x`.
2. Press `Enter`.

   For more information on the **status nr-registration survivable-processor node-name x** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Network design notes for the Split Registration Prevention feature

Ensure that you fulfill the following requirements when you administer split registration prevention:

- Run the **disable nr-registration** command in a region that has gateways. The survivable server becomes active when a gateway registers itself to the server. The main server deactivates all regions backed up by the survivable server.
- If the survivable server associated with the region is active, run the **enable nr-registration** command to auto disable the network region.
- You cannot use the **enable nr-registration** command to activate a network region that is automatically deactivated by the Split Registration Prevention feature.
- All gateways must have trunks and VoIP resources. The branch gateways registered to the survivable server that do not have trunks and VoIP resources are the only ones registered to a survivable server. This is similar to the situation when G650 media gateways without trunks and VoIP resources are the only port networks controlled by a survivable server.
- If the processor Ethernet addresses of survivable server are listed in a telephone Alternate Gatekeeper List (AGL) or Media Gateway Controller (MGC) list, split registrations might occur between the main server and the survivable server. Administrators can include C-LANs controlled by the survivable server in AGLs. If a telephone registers to a C-LAN controlled by a survivable server, the telephone can make calls with the trunk.
- When administering the MGC list of a media gateway, the part of the list after the survivable server transition point must contain only one entry administered under the **BACKUP SERVERS** heading of the Media Gateway region on the IP Network Region screen.
- If the corresponding survivable server is currently registered and active, you cannot change a survivable server entry under the column heading **BACKUP SERVERS IN PRIORITY ORDER**.
- All gateways in a single network region using time-day-window media recovery rules must follow the same rule. Any variation to the recovery rules creates confusion about further events.
- The AGL that IP telephones receive after they reboot must contain the address of the survivable server at the end of the list. If the IP address of the survivable server is not listed in AGL and the main server is unreachable, telephones cannot register with the survivable server.

Network region type description

When you administer a survivable server as a backup server for one or more network regions, the survivable server can have resources from one or more network regions. When the main server receives the status of the survivable server as active, the status of the network regions change to auto-disable (ad). The system can automatically activate network regions and the telephones and gateways can automatically register with the main server at the configured time and date.

To display the status of all the network regions and gateways in those regions, run the **status nr-region** command.

To change the status of a network region to manually disabled (rd), run the **command disable nr-registration**. To activate a network region, run the **enable nr-registration** command.

When a Survivable Remote Server reports active to the main server, the main server changes the status of those regions to auto disable (ad). This happens if any of the regions with the SRS backup server were manually disabled on the main server.

For more information on the **status nr-region** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Prerequisites and constraints of implementing the Split Registration Prevention feature

The main server and the survivable server, either SCS or SRS, must have Communication Manager Release 5.2 or a later release.

The main server and the survivable server must have an identical release of Communication Manager installed.

To administer split registration prevention, the following conditions must be met:

- On the Systems Parameters Media Gateway Automatic Recovery Rule screen, set the **Migrate H.248 MG to primary** field to **time-day-window**. You can also set this field to either `immediate` or `none` when no other gateways are using the rules
- After implementing the Split Registration Prevention feature, the **BACKUP SERVERS IN PRIORITY ORDER** column on the IP Network Region screen must have only one entry for the survivable server. The number of non-survivable server entries in this column is not affected.

Administrable Alternate Gatekeeper List for IP phones

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

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

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

The H.323 telephones use the AGL when they cannot reach or register with their primary gatekeeper. H.323 telephones use the AGL list of C-LANs or PE for recovery when the current C-LAN is no longer available. The Survivable Remote Servers can 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 six Survivable Remote Servers and one survivable gateway. This is true whether or not the region of the telephone is using the Administrable AGL feature. Without AGL, the number of nonsurvivable IP interface addresses in the network region depends on several factors:

- If the current Ethernet interface is a C-LAN interface of 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.

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 to each destination region. The total AGL assignments for each region must add up to 16 or lower. If 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 is administered to have only three 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 changes to the AGL fields and enters new values.

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

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*. For more information about the **Gatekeeper Priority** field, see Load balancing for PE.

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 commonly available C-LAN within the IP (H.323) telephone 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 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. The system checks all directly connected regions 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. The system also checks indirect network regions beginning with network region 1.

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

Load balancing for non-TTS telephones is based on the C-LAN received in GCF. Non-TTS telephones use this C-LAN to initiate a registration request (RRQ), and establish a socket to Communication Manager after completing Registration Admission Status (RAS).

Socket load balancing for TTS telephones occurs after registration is complete and AGL has been formed. Communication Manager initiates socket establishment to TTS telephones. Load balancing occurs across the C-LANs that were sent in AGL. Direct network regions and indirect network region C-LANs are considered as two groups.

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

How Alternate Gatekeeper List is built

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

1. 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.
2. The system then builds the AGL based on the list of administered directly connected regions. The order of regions is selected by round robin method, and the C-LANs are selected based on the same random algorithm that is used for selecting C-LANs from the home region.
3. The system builds 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 IP (H.323) telephone can now use C-LANs from all network regions as alternate gatekeepers, as long as they are connected (directly or indirectly) to the native region. The alternate gatekeepers are sent in the following order: in-region, directly connected regions, and indirectly connected regions.

Applications for AGL

This section describes the two common issues addressed by the administrable Alternate Gatekeeper List (AGL) feature of Communication Manager.

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

- Example 1 shows how to ensure that the IP telephone does not receive unwanted C-LANs in AGL. The example also shows an improved configuration for this issue.
- Example 2 shows how pooling C-LANs in a network region results in some IP telephones not receiving an AGL. The example also shows the improved configuration for this issue.

Prevent unwanted C-LANs in the AGL example

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

The figure on page 74 shows how unwanted C-LANs can end up in the Alternate Gatekeeper List.

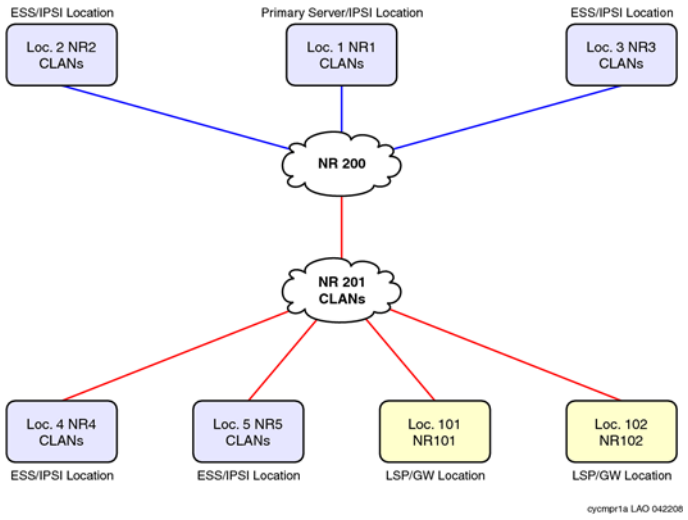


Figure 1: Unwanted C-LANs in Pre-Communication Manager 5.1 AGL

In this configuration, the IP telephones in NR1 through NR3 have C-LANs in their network regions as there are no C-LANs that are directly connected to NR200. You can add a few C-LANs in NR200 to share with NR1-NR3 as they are directly connected. NR 200 consolidates traffic from NR1-NR3 to obtain access to WAN. Using NR 200 also isolates C-LANS in each network region to IP telephones in that particular network region.

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

NR101 and NR102 are Gateway or Survivable Remote Server locations and should share pooled C-LANS. In this case, C-LANS are placed in NR201 as it is directly connected to the two NRs. These C-LANs are physically at the main location. Before Communication Manager Release 5.1 C-LANs could be in home region of the IP Phone or in a directly connected NR. The IP telephones in NR101 and NR102 now receive AGL information that contain C-LANs from NR201.

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 in recovering to a Survivable Core Server.

The figure on page 75 shows a workaround supported on Communication Manager 5.1 and earlier. You can implement this workaround using another virtual network region.

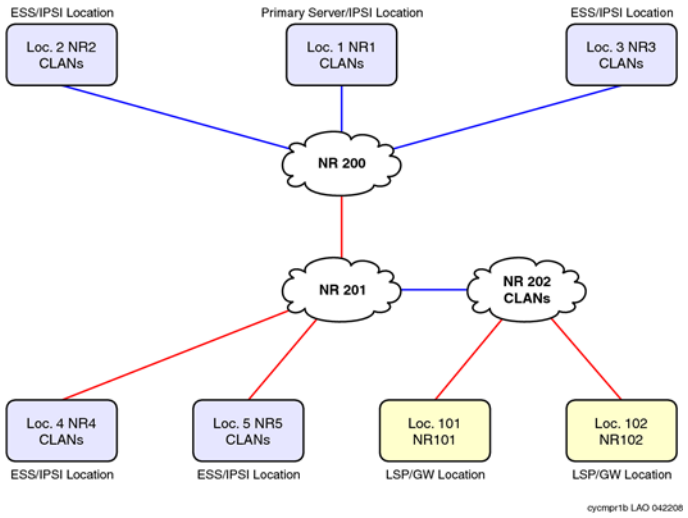


Figure 2: Pre-CM5.1 workaround for unwanted C-LANs

In this configuration, the IP telephones in NR4 and NR5 use the IP network map for NR assignment. 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. These C-LANs are physically located at location 1. If there are a large number of C-LANs in NR202, it could result in large AGLs and potentially delay recovery to the Survivable Core Server. This workaround does not address the size of the AGL.

The figure on page 76 shows the improved configuration of the network region using the Administrable AGL feature for Communication Manager 5.1. The IP Telephones in NR4 and NR5 receive C-LANs only in NR4 and NR5 respectively. The IP Telephones in NR101 and NR102 receive C-LANs only in NR201.

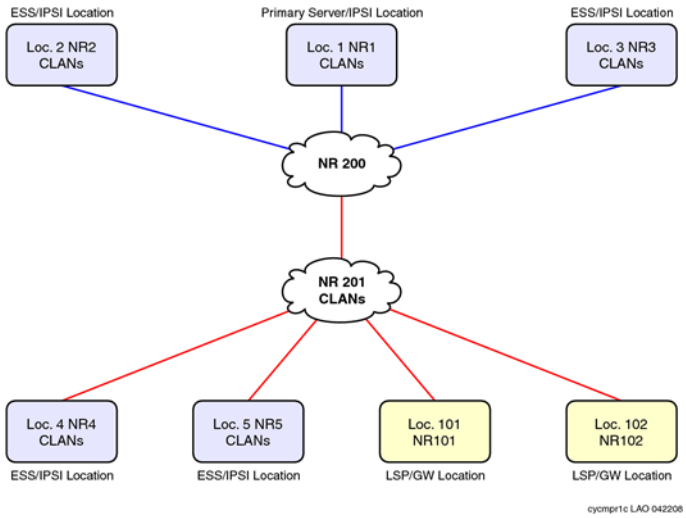


Figure 3: Improved configuration for unwanted C-LANs using the enhanced AGL feature

The figure on page 76 shows the 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. A large number of C-LANs in NR201, might result in large AGLs, and delay recovery to the Survivable Core Server.

With this enhancement, administrators can specify the number of C-LANs in NR201 and control the size of AGL.

Pool C-LANS despite network region connectivity issues example

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

The figure on page 77 shows how network region connectivity issues can prevent pooling of C-LANs.

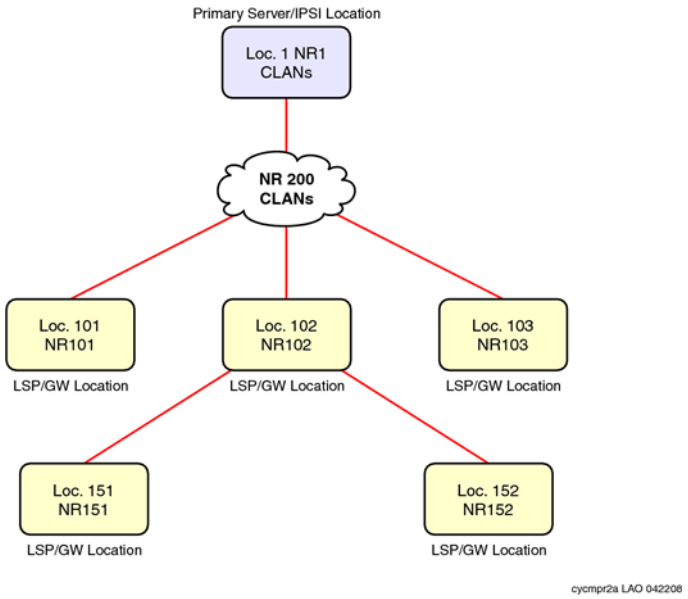


Figure 4: Inadequate pooling of C-LANs

The figure shows a network configuration with numerous gateway or survivable remote server locations, some of which are directly connected to the WAN, and others that are indirectly connected to the WAN. All these gateways need to share a pool of C-LANS located at location 1.

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

The figure on page 77 shows the workaround that you can use in the pre-Communication Manager 5.1 implementation.

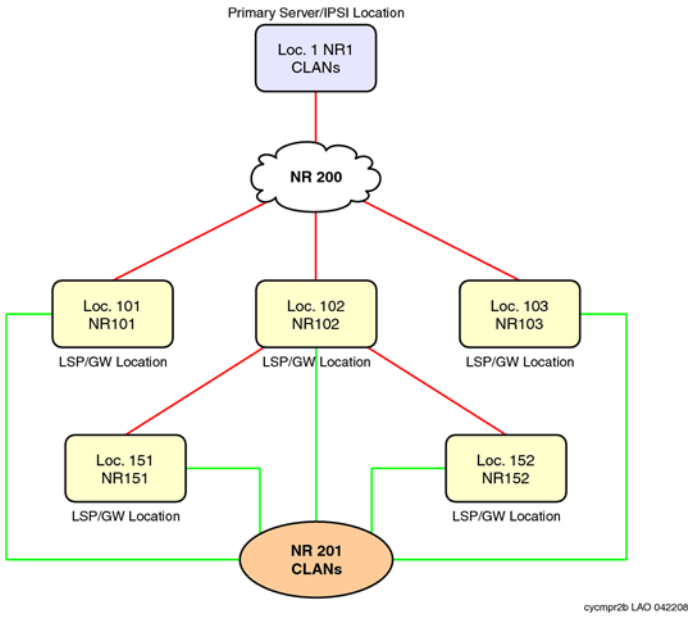


Figure 5: Pre-Communication Manager 5.1 workaround for inadequate pooling of C-LANs

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

The figure on page 78 shows the improved configuration using the Communication Manager 5.1 Administrable AGL feature.

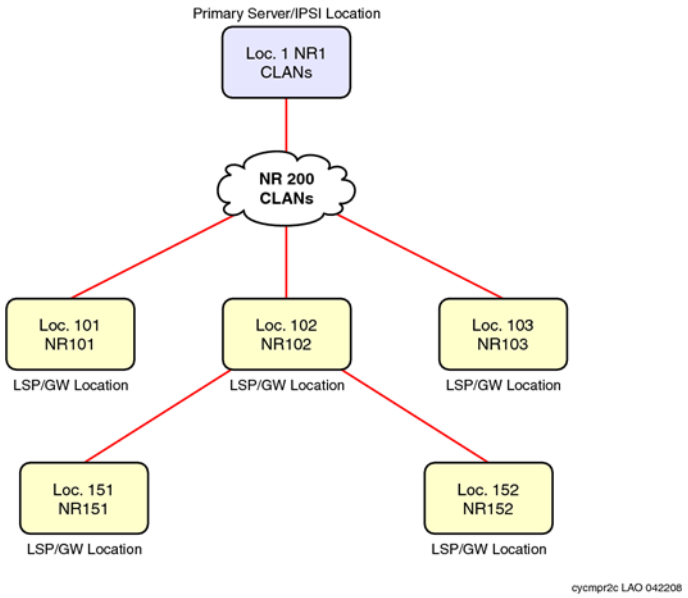


Figure 6: Improved configuration using the CM5.1 AGL feature

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

AGL high-level capacities

The total AGL assignments for each source region must add to 16 or lower. Each source network region can have six survivable remote servers from the telephone home region to be added to AGL. This brings the total list size to a maximum of 23 by adding AGL, survivable remote server for each region, and the survivable gatekeeper for the station.

Considerations

If the telephone IP address is not in one of the ranges in the IP network map, the AGL entries consist of C-LANs or PE from the telephone home region only. Note that when administering an IP address of a telephone in a network map, the associated AGL works robustly by accessing connected regions and the homed region directly and indirectly.

Interactions

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

- You can have some regions that use the pre-Communication Manager 5.1 nonadministrable AGL implementation, and some other regions that use the new administrable AGL implementation. But you cannot have a single network region that use a combination of the two methods. The AGL column can either contain numbers or alphabets, but not both. The field can also contain blanks. Blanks are ignored by both the old and the new implementation of this feature.
- This feature only applies to H.323 IP telephone registrations and H.323 IP telephone AGLs. The H.323 gateways also register to Communication Manager. This feature does not affect how the gateways obtain and use their own lists of gatekeepers. This feature does not impact on how IP (SIP) telephones register to SM 6.0 or SES 5.2 and earlier.
- If an extension number has shared control using the server between an H.323 IP telephone and an H.323 IP softphone, Communication Manager displays both the AGLs that were sent to the H.323 telephone and H.323 softphone.
- In prior releases of Communication Manager, the AGL feature only included C-LANs from the same region and from directly connected regions. The AGL feature included C-LANs from all indirectly connected regions if there were no C-LANS in the same or directly connected regions. With this enhancement, it is now possible to explicitly administer Communication Manager to include C-LANs from indirectly connected regions as well. Also, if you administer a non-zero value in the AGL column for an indirectly connected region, it opens that indirectly connected region C-LANs to be eligible to be used for load balancing.
- In general, when using the Communication Manager 5.1 Administrable AGL feature, C-LAN priorities should not be used. Note the following information:
  - For TTS telephones, Communication Manager 5.1 enhanced feature considers priorities, C-LAN socket load, C-LAN’s service state, and whether the H.323 IP telephone registration can use C-LANs for 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 5.1 enhanced feature does not take either priorities or C-LAN socket load into consideration when building the AGL.

Administrable AGL administration

Use the following procedures to administer the Communication Manager Administrable AGL feature on your system:

Requirements

Procedure

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

Configuring Administrable AGL

Procedure

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

   The system displays the Inter Network Region Connection Management screen. Scroll down to the AGL column.

2. Check your settings for the AGL column.

   a. To use the Administrable AGL feature, enter a numeric value in the 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 AGL when a telephone registers in the source region.

      Note:

      You can 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 Release 5.0 or earlier version of this feature to determine AGL.

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

      In this case, set them to **all** or blank. Note that if the value for every row is **all** or blank, the system automatically uses the Release 5.1 or earlier version of this feature to determine AGL.

3. Select `Enter` to save your changes.

Viewing IP Network Maps

Procedure

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

Verifying AGL settings for stations

Procedure

1. Enter **status station** *xxxxx*, where *xxxxx* is the extension of the station registered to the region having a numeric value for its AGL, which means it is using the Administrable AGL feature.
2. Scroll to the Alternate Gatekeeper List page.

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

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

   The fields on this screen are read only. For more information about IP Network Region Screen and Station Screen, see *Avaya Aura® Communication Manager Screen Reference*.
3. Verify the information for your system.
4. Type `Enter` to exit the screen.

Troubleshooting scenarios and repair actions for AGL

Under the following circumstances, the Station screen, command: **status station**, sometimes shows a different AGL than the one in use.

- 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 information stored by the telephone is hidden from the system. 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 particular gatekeeper address to their local AGL copy.

Related Documents for AGL

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

- *Administering Network Connectivity on Avaya Aura® Communication Manager*
- *Avaya Aura® Communication Manager Screen Reference*
- *Avaya Aura® Core Solution Description guide*
- *Avaya Aura® Communication Manager Survivable Options*
- *Application Notes for Administrable Alternate Gatekeeper List for IP Phones Using Communication Manager*

Improved Port network recovery from control network outages

When the network fails, IP connected port networks experience long outages from short network disruptions. Improved Port network recovery from control network feature enables you to see IP connected port networks with less downtime in case of IP network failures.

When there is a network outage, port networks do a warm restart rather than a reset for 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 quickly return to normal after a network failure. 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 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 unavailable 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 or from announcements
- Calls transitioning to or from music-on-hold
- Calls on hold
- Calls in ACD queues
- Calls in vector processing

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

The following are additional improvements:

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

For more information on System parameters screen, see *Avaya Aura® Communication Manager Screen Reference*.

Impact of network recovery configuration on availability

Communication Manager reduces the downtime of port networks during a short network outage. In Communication Manager 5.2, the H.323 endpoint, the application link and the socket stability are enhanced in the sub-60 second range as compared to Communication Manager 5.1. H.323 endpoints using TTS do not regenerate sockets. H.323 endpoints that do not use TTS do not reregister or regenerate sockets.

Improved survivability administration

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

Call processing administration

The telephony features of server are administered using the same commands and procedures as in a duplicated server.

Communication Manager administration interface

You can access Communication Manager through SAT program.

System Access Terminal

System Access Terminal (SAT) program uses a Command Line Interface (CLI) interface for telephony administration.

Security considerations

Administration login passwords are passed in plain text with no encryption. The exceptions to this no-encryption policy include:

- The EASG program installed on all Avaya servers.
- An encrypted web interface to the Avaya server. See the security certificate information in the server online help.
- Optional encryption for data backups. See data backup and restore.
- Support for RADIUS authentication for gateways.

Command syntax changes for media modules

The syntax for using the SAT commands for a gateway or an Avaya 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 suit media modules, a new convention was developed. The numbering convention for media modules uses the same seven-character field as does a traditional system, however the fields represent the 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, 001 represents the gateway number, V2 represents the slot number (possibly V1 through V9), and 05 represents the port number.

Communication Manager SAT CLI access

You can access the CLI of the Communication Manager SAT using any of the following methods:

- Secure Shell remote login
- Using Telnet over the Customer LAN

Secure Shell remote login

Using Secure Shell (SSH), you can log in remotely to the following:

- Supported gateways
- Supported servers
- Communication Manager SAT interface on an Avaya common server using port 5022.

The SSH capability provides a secure method for remote access. For more information on supported servers and gateways, see *Avaya Aura® Communication Manager Hardware Description and Reference* guide.

Note:

You must set up the client device for remote login and configure the device for SSH. For information about understanding the relevant commands for SSH, see your client PC documentation.

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

About this task

Prerequisites:

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

Procedure

1. Enter `enable filexfr [board location].`
2. Enter a three-six alphabets as login in the **Login** field.
3. Enter a seven-eleven character password (one character must be a number) in the first **Password** field.
4. Re-enter the same password in the second **Password** field.
5. Set the **Secure?** field to `y`.
6. Select `Enter`.

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

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

Procedure

1. Enter `disable filexfr [board location]`

   SFTP is disabled on the circuit pack.
2. Select `Enter`.

Using Telnet over the customer LAN

Before you begin

Ensure that you have an active Ethernet (LAN) connection from your computer to the Communication Manager server.

About this task

Use Avaya Terminal Emulator or access the server CLI using an SSH client, such as PuTTY, and 192.11.13.6. IP address, instead of Telnet.

Procedure

1. To access the Telnet program:
   - On a Windows system, go to the **Start** menu, and click **Run**.
   - Type `telnet <server_IP_address> 5023`. You can type the server name if the DNS server of your company is administered with the Avayaserver name.
2. When the system displays the **`login`** prompt, type the appropriate user name, such as *cust* or *craft*.
3. When prompted, enter the password or EASG response.
   - If you log in as **`craft`**, you receive a prompt to suppress alarm origination.
4. Select the default value (yes).
5. Select your preferred terminal type.

Enabling transmission over IP networks for TTY and fax calls example

Before you begin

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

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

Procedure

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

   For more information about fax or TTY over IP, see *Administering Network Connectivity on Avaya Aura® Communication Manager*.

Administration screen and command summary

The following screens are used to administer Gateways, Avaya servers, and other media modules.

Communication Manager commands to administer gateways

Communication Manager SAT commands and screens to administer gateways include:

The Media-Gateway administration screen is used to administer 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, Branch Gateways and Servers*.

- Use the **`list media-gateway ['print' or 'schedule']`** command to list the currently administered gateways. Information includes the gateway number, name, serial number, IP address, and whether or not this gateway is currently registered with the call controller. The IP address field is blank until the gateway registers once, then remains populated.
- Use the **`list configuration media-gateway x`** command to list all the assigned ports on the media modules for the 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*.

- The OPTIONAL FEATURES section contains a **Local Survivable Processor** field. If it displays a y (yes), this Avaya Server is configured to provide standby call processing in case the primary server is unavailable. See Local Survivable Processor configuration on page 60 for details.

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

- - **Port Network Support**: set to **`n`** indicates that traditional port networking is disabled. An S8300E Server is the primary call controller.
  - **Processor Ethernet:** set to **`y`** indicates the presence of an S8300E.

Quality of Service Monitoring screens

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

- Using an RTCP MONITOR SERVER section on the IP-Options System Parameters screen you can enter a single default IP address, server port, and RTCP report period that can be used 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 more information about QoS monitoring, see *Administering Network Connectivity on Avaya Aura® Communication Manager*. 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 or DPT-related fields to developers and field support personnel.

Gateway serviceability commands

Additional commands related to gateways appear in *Maintenance Commands for Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*. These include:

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

Voice or Network Statistics administration

In Communication Manager Release 5.2, the Voice or Network Statistics feature provides voice and network related measurement data through the SAT interface to help you troubleshoot voice quality issues. The media processor board collects various data elements. The three elements

that are used to generate the voice quality measurement reports are **Packet Loss**, **Jitter**, and **RT Delay**.

Note:

The voice or network statistics feature supports only TN2302 or 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 or 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 or 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 or Network Thresholds** field set to y, their corresponding default value **Packet Loss**, **Jitter**, and the system displays the **RT Delay** fields on the IP Interface screen.

If you change the **Enable Voice or 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 or TN2602 board, the system displays the `Board must be a valid TN2302 or TN2602` error message.

If you change the **Enable Voice or 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, you must administer all boards for which you want to collect data on the Media Processor Measurement Selection screen.

You can generate the report to record the voice statistics for each of the threshold criteria and for the data calls at both an hourly and summary level. You can view this report at both a network

region and media processor board level. Report reflects data for up to 24 hours period. You can generate the following reports:

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

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

For more information on the voice or network statistics reports, see *Avaya Aura® Communication Manager Reports*.

SNMP administration

For more information, *Avaya Aura® Communication Manager SNMP Administration and Reference*.

CAC sharing between Communication Manager and Session Manager

Communication Manager can establish VoIP media for H.323 stations and trunks, for inter Port Network, gateway or Avaya Aura® Media Server IP connections and for non-Session Manager routed SIP trunks. These IP media connections are not visible to Session Manager. In Communication Manager 7.1, Session Manager can be configured as a central authority for bandwidth management. With this setting, Communication Manager requires bandwidth for voice and multimedia IP connections from Session Manager. You can set the bandwidth limits applicable for various locations through System Manager. For more information about setting bandwidth limits, see *Administering Avaya Aura® Session Manager*.

Network preemption

Communication Manager supports network preemption. For network preemption to work, Communication Manager must be configured to use Session Manager as the bandwidth manager. To configure Session Manager as the bandwidth manager, see *Avaya Aura® Communication Manager Feature Description and Implementation*. The security administrator can assign bandwidth budgets for audio and video, to each network link on Session Manager. When server or network resources are running too low to allow additional calls, call preemption occurs. For more information, see *Administering Avaya Aura® Session Manager*.

Support to tandem MIME for PIDF-LO

Communication Manager Release 7.1.1 and later can tandem Multipurpose Internet Mail Extensions (MIME) attachments for Presence Information Data Format Location Object (PIDF-LO) in a SIP message. Communication Manager can also pass the PIDF-LO information in the SIP message.

Support for Channel Type identification over ASAI to CTI application

Communication Manager Release 7.1.1 supports channel type identification over ASAI to a CTI application. For incoming SIP trunk calls, Communication Manager Release 7.1.1 identifies the channel type as voice, video, or unknown when the call:

- Enters a monitored Vector Directory Number (VDN) or hunt group (skill/split).
- Is monitored and is alerting at a deskphone or Agent.

For this feature to work, the CTI link between Communication Manager and Application Enablement Services must be greater than 7.

This feature might not work or might show an unknown channel type on the CTI application when:

- The Direct Media feature is enabled.
- Communication Manager is not able to identify the channel from the incoming SIP request.

Chapter 5: Processor Ethernet setup

Processor Ethernet (PE) provides connectivity to IP endpoints, gateways, and adjuncts. The PE interface is a connection in the Communication Manager software that uses a port on NIC in the server. No additional hardware is required to implement PE, but the feature must be enabled using a license file.

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

Note:

The PE interface is enabled automatically on a survivable remote or a survivable core server. If the PE interface is disabled, the survivable remote or survivable core server cannot register with the main server and becomes nonfunctional.

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

The capabilities of survivable core servers are enhanced to support the connection of IP devices to the PE interface and to C-LAN interfaces located in G650 Media Gateway.

Note:

When you use PE on duplicated servers, you can use the following IP telephone models to ensure an optimal system performance:

- 9610, 9620, 9630, 9640, and 9650 telephones with firmware 3.0 or later, or any future 96xx and 96x1 models that support Time to Service (TTS) to 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 reregister in case of server interchange. If not in the same subnet, the 46xx telephones reregister as the servers.

When PE is used on duplicated servers, PE must be assigned to an active server IP address. The active server IP address is shared between the servers. In networking technology, this address is called IP-alias. The active server is the only server that responds to the IP-alias.

A survivable remote or a single survivable core server can use the PE interface to connect to CDR, AESVCS, and CMS. Duplicated survivable core servers can use the PE interface to connect to CDR, Messaging, and SIP Enablement Server (SES).

For more information about survivable core servers, see *Avaya Aura® Communication Manager Survivable Options*.

Setting up the PE interface

About this task

This section contains general and high-level steps for configuring and administering the PE interface. As each system has unique configuration requirements, refer to the Avaya Support website at http://support.avaya.com for more details.

Procedure

1. Load the appropriate template.
2. Configure the PE interface on the server using the server System Management Interface (SMI).

   See Configuring the PE interface on the server using the server SMI.
3. On the IP Node Names screen on the Communication Manager System Access Terminal (SAT), enter the name for each survivable core server, survivable remote server, and adjunct.

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

   On some platform types, the IP Interfaces screen is already configured.

   Use the SAT command **`display ip-interfce procr`** to see if the PE interface is already configured. If it is not, use the SAT command **`add ip-interface procr`** to add the PE interface.
5. Use the Processor Channel Assignment screen (command **`change communication-interface processor-channels`**) and the IP Services screen (**`change ip-sevices`**) to administer the adjuncts that use the PE interface on the main server:
   - Enter `p` in the **Interface Link** field on the Processor Channel Assignment screen.
   - Enter `procr` in the **Local Node** field on the IP Services screen.

6. For adjunct connectivity to a survivable core server or survivable remote server, use the Survivable Processor - Processor Channels screen to:
   - Use the same processor channels information as the main server by entering `i(nherit)` in the **Enable** field.
   - Use different translations than that of the main server by entering `o(verwrite)` in the **Enable** field. After entering `o(verwrite)`, you can enter information specific to the survivable core server or survivable remote server in the remaining fields.
   - Disable the processor channel on the survivable core server or survivable remote server by entering `n(o)` in the **Enable** field.
7. Execute a **`save translations all`**, **`save translations ess`**, or **`save translations lsp`** command to send (file sync) the translations from the main server to the survivable core server or survivable remote server.

Related links

Configuring the PE interface on the server using the server SMI on page 95

Configuring the PE interface on the server using the server SMI

About this task

Use the following procedure to configure the PE interface on the server using the server SMI.

Procedure

1. Select the interface used for PE on the Network Configuration page.

   S8300E provides only one interface to configure PE.

   The Network Configuration page can be found on the server's SMI. Select **Server (Maintenance)** > **Server Configuration**.
2. If this is a survivable core server or a survivable remote server, enter the additional information in the Configure LSP or ESS screen.
   - **Registration address at the main server** field: Enter the IP address of a C-LAN or PE interface on the main server to which the survivable remote server or survivable core server connects. The IP address is used by the survivable remote server or survivable core server to register with the main server. In a new installation where the survivable remote server or the survivable core server has not received the initial translation download from the main server, this address is the only address that the survivable remote server or the survivable core server can use to register with the main server.
   - **File synchronization address of the main cluster**: Enter the IP address of a server's Network Interface Card (NIC) connected to a LAN to which the survivable remote server or the survivable core server is also connected. The survivable core server or the

survivable remote server must be able to ping to the address. Select which interface you want the file sync to use. Use the customer LAN for file sync.

Using Network ports

The main server(s), Survivable Remote Servers and each Survivable Core Server use specific TCP or UDP ports across a customer's network for registration and translation distribution. The following Table 1: Network port usage on page 96 provides information to determine which TCP or UDP ports must be open in your network for a Survivable Remote or Survivable Core Server. Check the firewalls on your network to open the required TCP or UDP ports.

Table 1: Network port usage

Port	Used by	Description
20	ftp data	
21	ftp	
22	ssh/sftp	
23	telnet server	
68	DHCP	
514	Used in Communication Manager 1.3 to download translations.	
1719 (UDP port)	The survivable servers to register to the main servers	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	

Table continues…

Port	Used by	Description
21873 (TCP port)	The main server(s) running Communication Manager 2.0 to download translations to the Survivable Remote Server(s)	Prior to an upgrade to Communication Manager 3.0 or later, servers running Communication Manager 2.x used port 21873 to download translations to the Survivable Remote Server(s). Once the upgrade to 3.0 is complete and all servers are running versions of Communication Manager 3.0 or later, the main server(s) uses port 21874 to download translations and port 21873 is no longer needed.
21874 (TCP port)	The main servers to download translations to the survivable servers.	A main server(s) uses port 21874 to download translations to the Survivable Core Server (s) and the Survivable Remote Server(s) on Communication Manager 3.0 and later loads.

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

Configuration of the PE interface

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

Network Configuration

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

Note:

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

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

- If the configuration setting for a field is blank, you can configure that setting from the Network Configuration page.
- If the configuration setting for a field is already obtained from an external source, such as Avaya Aura® System Manager Solution Deployment Manager, that field is view-only.

- If you want to change the configuration setting obtained from an external source, you must navigate to the external source, such as Avaya Aura® System Manager Solution Deployment Manager used to configure the settings.

You can also configure the IP-related settings for each Ethernet port to determine how each Ethernet port is to be used (functional assignment). Typically, you can configure an Ethernet port without a functional assignment. However, any Ethernet port intended for use with Communication Manager must be assigned the correct functional assignment. Make sure that the Ethernet port settings in the Network Configuration page match with the physical connections to the Ethernet ports. Ethernet ports can be used for multiple purposes, except for the service's laptop port. However, currently there is no laptop service port within Communication Manager.

The number of entries for the Ethernet ports in the Network Configuration page corresponds with the number of Network Interface Cards (NICs) the server has.

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

Important:

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

Duplication parameters

Communication Manager supports two server duplication types:

- software-based duplication
- encrypted software-based duplication

Note:

The server duplication type must be the same for both the active and standby servers.

Duplication parameters of the other server include the host name, server ID, corporate LAN IP address, and duplication link IP address for the other server.

PE parameters include configuring the printer change priority level for the server and the IP address. The IP address facilitates the server to determine whether the PE interface is working or not.

To activate the new settings in the server, you must restart Communication Manager. Restart Communication Manager only after configuring the complete settings of the server. Several restarts can escalate to a complete Communication Manager reboot.

See the Duplication parameters page to configure the following settings for the server.

PE Interface acceptance test

Scenario	Acceptance criteria	Outcome	Verification parameters for the wanted outcome
Main server is duplicated and PE interface is not used	PE interface is not enabled (no ESS server is provided and no IP endpoints are controlled by PE interface)	Status Summary page shows: • PE connection is not functional on both servers • PE connection is not functional on both servers	For Communication Manager 5.0 and 5.1 releases: • PE Interface is set to UNUSED on the Set Identities page • PE Interchange Priority is set to IGNORE on the Configure Interfaces page For Communication Manager 6.0 and later releases: • Functional Assignment for eth0 does not include PE on the Network Configuration page • PE Interchange Priority is set to IGNORE on the Duplication Parameters page

Table continues…

Scenario	Acceptance criteria	Outcome	Verification parameters for the wanted outcome
Main server is duplicated and PE interface is used	PE Interface is enabled on the main server and the ESS server (either ESS server is provided or IP endpoints are controlled by PE interface, or both)	Status Summary page shows: • PE connection is not functional on both servers • PE priority is set to the same value (but not IGNORE) for both servers	For Communication Manager 5.0 and 5.1 releases: • PE Interface is set to one of the Ethernet interfaces on the Set Identities page • PE Interchange Priority is set to the same value (but not IGNORE) on the Configure Interfaces page on both servers For Communication Manager 6.0 and later releases: • Functional Assignment for eth0 includes Processor Ethernet on the Network Configuration page • PE Interchange Priority is set to the same value (but not IGNORE) on the Duplication Parameters page on both servers
Either the main server or the ESS server is duplicated	–	Current Alarms page (or running almdisplay -v on the command prompt) shows no active _PE alarms for up to 15 minutes after both servers have been running as an active or standby pair	–

Configuring a Survivable Remote or Survivable Core Server

About this task

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

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

Procedure

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

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

   The Survivable Core or Survivable Remote Server must be able to ping to the address. Select the interface you want the file sync to use. Use the customer LAN for file sync.

PE as a controller for branch gateways

About this task

Use the command **`set mgc list`** on a branch gateway while adding a PE-enabled S8300E as a primary controller or as an alternate controller. The primary controller or gatekeeper is the first gateway controller on the list.

For example, an NIC card with IP address 132.222.81.1 is chosen for the PE interface during configuration. The **`set mgc list`** command is:

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

PE in Communication Manager Administration

Processor Ethernet administration is always performed on the main server. The Survivable Remote or Survivable Core Server receives the translations from the main server during

registration or when you perform a **save translations lsp**, **save translations ess**, or **save translations all** command on the SAT of the main server.

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

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

- IP Node Names screen

  If the PE interface is enabled in the license file, the system displays the PE interface (`procr`) automatically 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 server is S8300E and for one or more of the following entities, use the PE interface of the main server to register with the main server:

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

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

- Survivable Processor screen

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

Administering Survivable Core Servers for PE

If there is a Survivable Core Server in the configuration, you must add the Survivable Core Server using the Survivable Processor screen. For more information on administering the Survivable

Core Server on the Survivable Processor screen, see *Avaya Aura® Communication Manager Survivable Options*.

Administering Survivable Remote Servers for PE

You can administer Survivable Remote Servers using the Survivable Processor screen. For more information on administering a Survivable Remote Server, see *Avaya Aura® Communication Manager Screen Reference*.

Adjuncts with PE

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

- **Survivable CMS**

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

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

- **CDR**

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

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

- **AESVCS**

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

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

Load balancing for PE

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

Note:

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

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

1. Load balancing starts with placing the C-LANs and the PE interface into a network region using the **Network Region** field.
2. Within the network region, further load balancing is done by entering a priority in the **Gatekeeper Priority** field. The system displays this field 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 `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 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.

Chapter 6: Manage telephones

Related links

Connecting new telephones on page 106

Installing new telephones

About this task

You can start a new telephone service by plugging in the telephone into a jack and dialing a sequence of numbers. The dialing sequence sets up an association between the telephone and the corresponding station administration.

Security alert:

The unauthorized use of this feature can cause security problems. For suggestions on how to secure your system and to obtain additional security information, see *Avaya Products Security Handbook*.

Procedure

1. On the Feature-Related System Parameters screen, ensure that the **Customer Telephone Activation (CTA) Enabled** field and the **TTI Enabled** field are both set to y.
2. Complete the Station screen for the new telephone, and type x in the **Port** field.

Note:

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

Caution:

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

Associating a telephone with an x-port extension number

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

Procedure

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. Disconnect after you receive the 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.

   Repeat the process until all new telephones have been installed.
6. For security reasons, disable the activation feature when you have activated your telephone. To do this, type change system-parameters features at the system administration terminal.
7. On the Feature-Related System Parameters screen, type `n` in the **Customer Telephone Activation (CTA) Enabled** field.
8. Press `Enter` to save your changes.
9. Type **`save translations`**.
10. Press `Enter` to permanently save the changes.

    Note:

    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.

Connecting new telephones

Before you begin

Ensure that you have the following:

- Port to use for the new telephone.
- Type of telephone to install.
- Location where you want to install the telephone.

Procedure

1. Find an available port.
2. Connect the port to the cross-connect field or termination closet.
3. Type the telephone details in the system.

Related links

Manage telephones on page 105

Gathering necessary information

Procedure

1. Determine whether the telephone is an analog, digital, ISDN, or a hybrid set. You can also administer a virtual telephone which exists without hardware at the time of administration. You need the information to determine the type of port you need because the port type and telephone type must match.
2. If you do not know what type of telephone you have, see the **Type** field on the Station screen for a list of telephones by model number.
3. Record the room location, jack number, and wire number.

   The information can be found on the jack where you want to install the telephone, in your system records, or from the technician doing the installation.
4. To view a list of boards on your system, type `list configuration station`.

   The available boards or cards and ports appear.
5. Press `Enter`.

   The System Configuration screen appears showing 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 the port of each board.
6. Choose an available port, and record its port address.

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

   Note:

   If you add several telephones at one time, you might want to print a paper copy of the System Configuration screen.
7. To print the screen to a printer attached to the system terminal, type `list configuration station print`
8. Press `Enter`.

9. To print to the system printer that you use for scheduled reports, type `list configuration station schedule immediate`.
10. Press `Enter`.
11. Choose an extension number for the new telephone.

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

Telephone installation

After reading the relevant information about how to connect a telephone, you are ready to connect the port to the cross-connect field. You can configure the system to set up the new telephone.

To request Avaya to install the new connections, go to the Avaya Support website at http://support.avaya.com. Notify the Avaya technical support representative or on-site technician that you are ready to add the telephone to the system.

If you are making the connections yourself, see the system installation guide for any questions.

Obtaining display labels for telephones

About this task

Download telephone display labels for each telephone type that you install.

Procedure

1. On the Station screen, set the **Display Language** field to English, Spanish, Italian, French, user-defined, or Unicode.

   Note:

   The Unicode display is only available for Unicode-supported telephones. Currently, the 4610SW, 4620SW, 4621SW, and 4622SW, 16XX, 96X1, and 96x0-series Spice telephones support Unicode display. Unicode is also an option for the 2420J telephone when **Display Character Set** on the System Parameters Country-Options screen is Katakana. For more information about 2420J, see *2420 Digital Telephone User's Guide, 555-250-701.*

2. On the System-Parameters Country-Options screen, set the **Display Character Set** field to one of the following for the 2420 or 2410 telephone.
3. On the Katakana for a Katakana character display.

Adding a new station

Before you begin

Ensure that the extension number you use conforms to your dial plan.

About this task

The information that you enter on the Station screen indicates that the telephone exists and connects the features you want to enable on the telephone. With Communication Manager, you can enter extensions with punctuation on the command line. Punctuation is limited to hyphens and periods. Communication Manager cannot process a command, such as `add station 431 4875`. You must format a command as one of the following:

- Add station 431-4875
- Add station 431.4875
- Add station 4314875

Procedure

1. To access the Station screen for the new telephone, do one of the following:
   - Type `add station nnnn` where nnnn is the extension for the new telephone.
   - Type `add station next` to automatically use the next available extension number.
2. **(Optional)** If you have **Terminal Translation Initialization (TTI)** enabled, you might receive the following error message when attempting to add a new station:

If you receive an error message:

```
No station/TTI port records available; display capacity for their
usage
```

Do one of the following:

3. Remove any DCP or analog circuit packs that have no ports administered on them.
4. Check if you are 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 if you are not using these features.

   Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to the topic, or to open a service request. For more information on TTI, see Terminal Translation Initialization in *Avaya Aura® Communication Manager Feature Description and Implementation* Guide, 555-245-205.

   For more information about the System Capacity screen, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

   By default, port 1720 is turned off to minimize denial of service situations on all IP softphones Release 5.2 and later. You can change this setting if you have root privileges on the system by typing the command: `/opt/ecs/ sbin ACL 1720 on` or `off`.
5. Press Enter. When the system displays the Station screen, you see the extension number and some default field values.

   The name you enter displays on called telephones that have display capabilities. Some messaging applications, such as INTUITY, recommend that you enter the last name of the user and their extension to identify the telephone. The name entered is also used for the integrated directory.

Tip:

To hide a name in the integrated directory, enter two tildes before the name when you assign it to the telephone. Set **Display Character Set** on the System Parameters Country-Options screen to Roman. The tildes are not displayed with caller ID name. Also, if a name is entered with only one tilde, the name is converted to Eurofont characters.

Note:

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

The name you enter displays on called telephones that have display capabilities. Some messaging applications, such as INTUITY, recommend that you enter the last name of the user and their extension to identify the telephone. The name entered is also used for the integrated directory.

Tip:

To hide a name in the integrated directory, enter two tildes before the name when you assign it to the telephone. Set **Display Character Set** on the System Parameters Country-Options screen to Roman. The tildes are not displayed with caller ID name. Also, if a name is entered with only one tilde, the name is converted to Eurofont characters rewrite in active voice

Note:

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

6. Press Enter to save your changes.

Creating a dual registered extension

About this task

With the SIP and H.323 dual registration feature, you can assign the same extension to H.323 and SIP endpoints.

Procedure

1. Through System Manager, create an extension of H.323 set type.

2. On the SAT screen, type `change off-pbx-telephone station-mapping n`, where *n* is the extension that you added through System Manager.
3. On the Stations With Off-Pbx Telephone Integration screen, add an `OPS` entry.

Changing a station

About this task

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

Procedure

1. Enter `change station nnnn` where *nnnn* is the extension of the new telephone.
2. Change the necessary fields as described in the previous section, and then press **Enter**.

Duplicating telephones

About this task

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

Note:

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

Procedure

1. Type `display station nnnn`, where nnnn is the extension of the Station screen you want to duplicate to use as a template.
2. Click `Enter`.
3. Verify that this extension is the one you want to duplicate.
4. Press `Cancel` to return to the command prompt.
5. Type `duplicate station nnnn`, where nnnn is the extension you want to duplicate. Then click `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. Count

<1-16> represents the number of consecutive extensions after the start extension to create duplicates.

Note:

You might want to duplicate the settings of another station where you need to change the port or station type. You must individually administer each station after creating the duplicates.

6. Type the extension, port address, and telephone name for each new telephone you want to add.

   The rest of the fields on the Station screen are optional. You can complete them at any time.

7. Click `Enter`.

   Changes are saved to system memory.

8. To make changes to these telephones, such as assigning coverage paths or feature buttons, type `change station nnnn`. nnnn is the extension of the telephone that you want to modify. Then press `Enter`.

Adding multiple call center agents

About this task

You can add multiple call center agents, all with the same settings, based on an agent that is already administered.

Procedure

1. Enter `command duplicate agent-loginID` on the CLI screen and the extension of the agent you want to duplicate.
2. Select `Start` and enter the extension you want to use for the first new agent.
3. Select `count` and the number of agents you want to add.
4. On the Agent LoginID screen, fill in the required information.

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

Using an alias

About this task

Not every telephone model or device has a unique Station screen in the system. You might have to use an available model as an “alias” for another. If you need to enter a telephone type that the system does not recognize or support, use an alias. Defining aliases is also a useful method to identify items that act as analog stations on Communication Manager, such as fax machines, modems, or other analog device.

If you purchase a telephone model that is newer than your system, you can alias this telephone to an available model type that best matches the features of your new telephone. See your telephone 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, you can create two aliases: one to add a new 6220 telephone and one to add modems to your system.

Procedure

1. See your new telephone manual to find the correct alias.

   To add a new 6220 telephone, you can find that the 6220 should be administered on an older system as a 2500 telephone. To do this:

2. Type `change alias station` on CLI.
3. Press `Enter`.

   The system displays the Alias Station screen.

4. In the **Alias Set Type** field, type `6220`.

   This is the name or model of the unsupported telephone.

5. In the **Supported Set Type** field, type `2500`.

   This is the name or model of the supported telephone.

6. In the **Alias Set Type** field, type `modem`.

   You can call the alias set anything you like. Once you define the alias, you can use the alias set in the **Type** field on the Station screen.

7. In the **Supported Set Type** field, type `2500`.

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

8. Press `Enter` to save your changes.

   Now you can follow the instructions for adding a new telephone (or adding a fax or modem). Avaya Communication Manager now recognizes the new type (6220 or modem) that you enter in the **Type** field.

   Be sure to see your telephone manual for instructions on how to set feature buttons and call appearance buttons.

Note:

If you need to use an alias for a telephone, you might be unable to take advantage of all the features of the new telephone.

Customize your telephone

You can customize the settings on your personal telephone. You can add feature buttons to monitor or test the system, so that you can troubleshoot the system from your telephone.

To troubleshoot the system, you need a telephone with the following facilities:

- A large multi-button display, such as 8434D or 8410D
- The class of service with console permissions
- Feature buttons, such as:
  - ACA and security violations assigned to lamp buttons
  - Busy verify
  - Cover message retrieval button
  - Major or minor alarm buttons
  - Trunk ID buttons
  - Verify button

After you select a telephone, select the place for this telephone, for example, 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.

You can set up multiple telephones for testing applications and features before you provide them to users. You can have a telephone that represents each type of user telephone in your organization. For example, if you have four basic telephone templates each for executives, marketers, technicians, and other employees, you can test new features or options. You can have examples of each of these telephones and test options. After you are satisfied that a change works on the test telephone, you can make the change for all the users in that group.

Upgrading telephones

About this task

You can change the telephone type for a user without changing the location. You can access the Station screen for the extension and enter the new model number.

Note:

This method is used only if the new telephone type matches the existing port type, such as a digital telephone with a digital port.

For example, a user at extension 4556 who has a 7410+ telephone and wants to replace the phone with a new 8411D telephone.

Procedure

1. On the command line interface, type `change station 4556`.
2. Press **Enter**.

   The system displays the Station screen for 4556.
3. In the **Type** field, overwrite 7410+ with `8411D`.
4. Press **Enter**.

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

Swapping telephones

About this task

Moving a telephone from one location to another or swapping telephones between two locations is only possible if the two telephones are of the same type. Swapping telephones between two locations is possible if the telephones are both digital or both analog. You can use X ports to easily swap the telephones, A and B. Change port assignment of telephone A to X, change telephone port assignment of B to old port of A, and finally, replace the X on telephone A to old port of B.

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

Procedure

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

12. Press `Enter`.
13. Type `01C0516` in the **Port** field.

    This is the port that was assigned to extension 4575.
14. Update the **Room** and **Jack** fields.
15. Press `Enter` to save your changes.
16. Physically unplug the telephones, and move them to their new locations.

    When you swap telephones, the system keeps the old button assignments. If you are swapping to a telephone with softkeys, the telephone could have duplicate button assignments because soft keys have default assignments. You can check your button assignments and modify them as necessary.

Automatic Customer Telephone Rearrangement

Automatic Customer Telephone Rearrangement (ACTR) is an enhancement to Terminal Translation Initialization (TTI), Personal Station Access 25 (PSA), and Customer Telephone Activation (CTA). ACTR makes it easy to identify and move telephones from one location and to another 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 or 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 or 2410 telephone. ACTR uses the stored information and associates the telephone with the new port when the telephone is moved.

When you move a telephone, the telephone must be plugged into an AC outlet at the new location. A telephone with remote auxiliary power must be supplied remote auxiliary power at the new location. If this is not done, some optional adjuncts, such as an expansion module, do not operate.

⚠ Caution:

When a telephone is unplugged and moved to another physical location, the **Emergency Location Extension** field must be changed for that extension or the USA Automatic Location Identification database must be manually updated. If this is not done, the DID number sent to the Public Safety Access Point (PSAP) could send the emergency response personnel to the wrong location.

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

When you enter always or once in the **Automatic Moves** field on the Station screen, Communication Manager obtains the serial number from the telephone and records it to ACTR Move List. If you change the entry in the **Automatic Moves** field from always or once to no, Communication Manager removes the extension from the Move List.

How calls are processed during a move

When a telephone is unplugged while on a call, and a 6400 Serialized telephone or a 2420 or 2410 telephone that is administered for automatic moves is plugged into the port within 60 seconds, the following happens.

- Both extensions are placed in idle state.
- Active calls on either extension are dropped, unless the call is active on a bridged appearance at some other telephone.
- Held calls remain in a hold state.
- Any calls ringing on either extension instantly proceed to the next point in coverage or station hunting path, unless the call is ringing on a bridged appearance at some other telephone.
- User actions that were pending when the new telephone was plugged in are aborted.

You can use the `list station movable` command to keep track of extensions on the move list up to the maximum number specified on Communication Manager.

Using ACTR to move telephones

Before you begin

- Be sure the **TTI** field on the Feature-Related System Parameters screen is set to y.
- Before you move a telephone in your system, set the **TTI State** field to voice on the Feature-Related System Parameters screen.

About this task

As an example, to move a telephone to extension 1234:

Procedure

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

Terminal Translation Initialization

Use Terminal Translation Initialization (TTI) to merge an x-ported station with a valid port. Dial a TTI merge code, a systemwide security code, and the x-port extension from a telephone connected to that port. Using TTI, you can 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 to move the telephone and data module from office to office. You can separate a telephone from its port with TTI. Unplug the telephone from the jack, plug the telephone into a jack in another office, and merge the telephone to its new port with TTI.

For more information about setting the security code for each extension, see Setting up Personal Station Access.

Security alert:

Security problems can arise from unauthorized use of this feature. For example, someone who knows the TTI security code can disrupt normal business functions by separating telephones or data terminals. To prevent such disruption, change the TTI security code frequently. Remove the Feature Access Code (FAC) from the system when not in use. For more information about security aspects and new security developments, see the Avaya Products Security Handbook.

Merging an extension with a TTI telephone

Before you begin

Before you can merge a telephone, you must set the **TTI State** field to voice on the Feature-Related System-Parameters screen. You also must set the extension to match the port type of the TTI port making the merge request. For example, a digital telephone type can merge only to a port on a digital board.

About this task

For example, a digital telephone type can merge only with a port on a digital board. You can destroy your hardware if you attempt to connect an analog telephone to a digital port. You cannot use TTI to change a virtual extension.

To merge an extension with a TTI telephone, the steps are as follows:

Procedure

1. Dial the TTI merge FAC.
   - If the code is correct, you receive dial tone.
   - If the code is incorrect, you receive intercept tone.
2. Dial the TTI security code from the telephone you want to merge.
   - If the code is correct, you receive the dial tone.
   - If the code is incorrect, you receive the intercept tone.
3. Dial the extension of the telephone you want to merge.
   - If the extension is valid, you receive confirmation tone, which might be followed by dial tone.
   - If the extension is valid and you receive the intercept tone immediately following the confirmation tone, attempt the merge again.
   - If the extension is valid but the extension is being administered, you receive the reorder tone. Try the merge again later.
   - If the extension is invalid, you receive the intercept tone.
   - If the system is busy and cannot complete the merge, you receive the reorder tone. Try the merge again later.

- If the telephone has a download status of pending, you receive the reorder tone. Change the download status to complete, and try the merge again.

Using TTI to separate an extension from a telephone

Procedure

1. Dial the TTI separate FAC.
2. Dial the TTI security code.
   - If the code is correct, you receive the dial tone.
   - If the code is incorrect, you receive the intercept tone.
3. Dial the extension of the telephone to be separated.
   - If you have dialed the extension of the telephone currently merged with this telephone, you receive the confirmation tone.
   - If you have dialed the extension of the telephone currently merged with this telephone, but the extension is being administered, you receive reorder tone. Try the separation again later.
   - If you have not dialed the extension of the telephone currently merged with this telephone, you receive the intercept tone.
   - If the system is busy and cannot complete the separation, you receive the reorder tone. Try the separation again later.

Troubleshooting TTI

If you have difficulty in using TTI, review the following system restrictions.

Problem	Restriction
The **TTI Ports** field on the System Capacity screen (type display capacity) shows the number of TTI ports used in a server running Communication Manager.	This field shows only the number of TTI ports being administered. If a TTI exceeds the maximum number of ports, the port is not administered and cannot be added. In that case, a telephone cannot be added. For details on the System Capacity screen, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*. 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.

Table continues…

Problem	Restriction
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.
When you use this order, voice and then data (Set the **TTI State** field to voice and then set the **TTI State** field to data), you reduce the chance of a user trying to use TTI on a data-only terminal that does not have TTI port translation	This can happen when the number of telephones allowed by the system is twice the number of data terminals. For example, if the system limit for telephones is 15,000 and 7,500 for data, then when TTI was turned on for data first, only the first 7,500 unadministered ports would get TTI port translations.
When TTI is activated for the system, these actions take place	• If the **TTI State** field was previously activated but in a different state (such as, a voice to data state), the old TTI translations are removed and the new ones added on a board-by-board basis. • If the **TTI State** field is set to voice, then default TTI translations are generated for every unadministered port on all digital, hybrid, and analog boards. • 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 is removed in the system, and the ports return to an unadministered state.

Removing telephones

Before you begin

Before you physically remove a telephone from your system, check the telephone's status, remove it from any group or usage lists, and then delete it from the system's memory. For example, to remove a telephone at extension 1234:

Procedure

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

   The system displays the General Status screen.
3. Make sure that the telephone is in the following state:
   a. Plugged into the jack
   b. Idle and not receiving calls
   c. No messages waiting
   d. No active buttons, such as **Send All Calls** or **Call Forwarding**
4. Type `list groups-of-extension 1234`.
5. Press `Enter`.

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

   If extension 1234 belongs to pickup group 2, type `change pickup group 2` and delete the extension from the list.
8. Type `list usage extension 1234`.
9. Press `Enter`.

   The Usage screen shows where the extension is used in the system.
10. Press `Cancel`.
11. If the system displays the extension on the Usage screen, access the appropriate feature screen and delete the extension.

    If extension 1234 is bridged onto extension 1235, type `change station 1235` and remove the appearances of 1234.
12. Type `change station 1234`.
13. Press `Enter`.
14. Type `remove station 1234`.
15. Press `Enter`.

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

Tip:

Be sure to record the port assignment for this jack in case you want to use it again later.

16. If this is the correct telephone, press `Enter`.
    a. If the system responds with an error message, the telephone is busy or still belongs to a group.
    b. Press `Cancel` to stop the request, correct the problem.
    c. Enter `remove station 1234` again.
17. Remove the extension from voice mail service if the extension has a voice mailbox.
18. Type `save translations`.
19. Press `Enter` to save your changes

Note:

You do not need to delete the extension from coverage paths. The system automatically adjusts coverage paths to eliminate the extension.

Next steps

Now you can unplug the set from the jack and store it for future use. You do not need to disconnect the wiring at the cross-connect field. The extension and port address remain available for assignment at a later date.

Once you successfully remove a set, that set is permanently erased from system memory. If you want to reactivate the set, you have to add it again as though it were a new telephone.

Adding a fax or a modem

About this task

Connecting a fax machine or modem to your system is similar to adding a telephone, with a few important exceptions. To add a fax or a modem, see *Adding Telephones* in the above section.

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. To be able to create reports that indicate which stations are faxes or modem. For more information about aliasing, see *Using Alias*.

As an example, if you have already defined an alias for “fax” as a 2500 station type and want to add a fax machine to extension 4444, the steps are as follows:

Procedure

1. Type `add station 4444`.

2. Press `Enter`.
3. In the **Type** field, type `fax`.
4. In the **Port** field, type the port address.
5. In the **Name** field, type a name to associate with this fax.
6. Move to the **Data Restriction** field and type `y`.

   Entering y in this field prevents calls to and from this extension from being interrupted by tone signals. This is important for fax machines and modems as these signals can disrupt transmissions of data.
7. In the **Distinctive Audible Alert** field, type n.

   This eliminates the distinct 2-burst ring for external calls, which often interferes with the auto-answer function on fax machines or modems.
8. Press `Enter` to save changes.

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

Before you begin

The ability to transmit fax, modem, and TTY calls over IP trunks or LANs and WANs assumes that the endpoints sending and receiving the calls are connected to a private network that uses H.323 trunking or LAN connections between gateways and/or port networks. This type of transmission also assumes that calls can either be passed over the public network using ISDN-PRI trunks or passed over an H.323 private network to Communication Manager switches that are similarly enabled. As a result, it is assumed that you have assigned, or will assign, to the network gateways the IP codec you define in this procedure. As an example, assign codec set 1 to the network region to enable handling of fax, modem, and TTY calls.

Procedure

1. Type `ip-codec-set 1` or `change ip-media-parameters 1`.
2. Press `Enter`.

   The system displays the IP MEDIA PARAMETERS screen.
3. Complete the fields as required for each media type you want to enable.
4. Press `Enter`.

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

IP Softphones

Using Avaya IP Softphones, the end user can control telephone calls directly from a Personal Computer (PC). An end user can log in remotely to the company server running Communication Manager, and then make and receive telephone calls from the telephone extension.

Avaya IP Softphones support the following modes:

- **Road-Warrior**

  You typically use this mode for laptop users who are travelling. In this mode, the Personal Computer LAN connection carries both the call control signaling and the voice path. Because the audio portion of the voice call is handled by the Personal Computer, you must have some kind of audio device (e.g., handset, headset) Personal Computer 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 Personal Computer audio application.

  The telecommuter mode uses the Avaya IP Softphone interface on the user Personal Computer and a standard telephone. The Avaya IP Agent mode uses the Avaya IP Agent interface on the agent Personal Computer and a call center telephone.

- **Native H.323 (only available with Avaya IP Softphone R2)**

  Using the standalone H.323 mode, the travelers can use some Communication Manager features from a remote location. This mode uses a Personal Computer 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 standalone H.323 users only features that they can activate with dial access codes.

- **Control of IP Telephone (only available with IP Softphone R4 and later)**

  You can use this mode 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. With this new configuration, an IP softphone and a non-softphone telephone can be in service on the same extension at the same time. Also, the call control is executed by both the softphone and the telephone endpoint, and the audio is monitored by the telephone endpoint.

Tip:

Use status station to show the part (product) ID, serial number, and the audio connection method used by existing stations.

Note:

Beginning with the November 2003 release of Communication Manager, R1 and R2 IP Softphone and IP Agent, which use a dual connect (two extensions) architecture, are no longer supported. R3 and R4 IP Softphone and IP Agent, which use a single connect (one extension) architecture, continue to be supported. This applies to the RoadWarrior and the Telecommuter configurations for the IP Softphone. Native H.323 registrations for R1 and R2 Softphones continue to be supported.

Enabling the system to use IP softphone

Procedure

1. Display the System Parameters Customer-Options (Optional Features) screen.
2. Verify the following field settings:
   - **Maximum Concurrently Registered IP Stations** is greater than 0.
   - **IP Stations** field is y
   - Information has been entered in the fields on the Maximum IP Registrations by Product ID page
3. Verify that your Communication Manager server has a Processor Ethernet board and a gateway.
4. Install the IP Softphone software on each IP Softphone user's Personal Computer.

Road Warrior Mode

Use Softphone in the Road Warrior mode when you want call control signaling and voice media to flow over the IP network between the softphone and Communication Manager.

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.

To illustrate, add a softphone in Road Warrior mode at extension 3001. Except for single-connect IP telephones, you have to actually administer two extensions for each Road Warrior mode.

Adding a Softphone in Road Warrior mode

Procedure

1. Type `add station 3000`.
2. Press `Enter`.

   The system displays the Station screen.
3. In the **Type** field, enter `H.323`.
4. Press `Enter` to save your work.

Administering Road Warrior

Procedure

1. Type `add station next`.
2. Press `Enter`.

   The system displays the Station screen.

   Note:

   To change an existing DCP extension, type `change station nnnn` in this step, where nnnn is the existing DCP extension.

3. In the **Type** field, enter the model of telephone you want to use.

   For example, enter `6408D`.

4. In the **Port** field, type `x` for virtual telephone, or enter the port number if there is hardware.

   Note:

   Port 1720 is turned off by default to minimize denial of service situations. This applies to all IP softphones release 5.2 or later. You can change this setting, if you have root privileges on the system, by typing the command: `/opt/ecs/ sbin ACL 1720 on` or `off`.

5. In the **Security Code** field, enter the password for this remote user.

   For example, enter `1234321`.

   This password can be 3-8 digits in length.

6. In the **Media Complex Ext** field, type `3000`.

   This is the H.323 extension just administered.

7. In the **IP Softphone** field, type `y`.
8. On page 2, in the **Service Link Mode** field, type `as-needed`.

   Set this field to `permanent` only for extremely busy remote telephone users, such as call center agents.

9. In the **Multimedia Mode** field, type `enhanced`.
10. Press `Enter` to save your work.

    Now you can install and configure the software on the user's Personal Computer. In this example, the user logs in by entering their DCP extension (3001) and password (1234321).

Adding a softphone in telecommuter mode

About this task

Use Softphone in telecommuter mode when you want call control signaling to flow over the IP network between the softphone and Communication Manager and voice media to flow over a telephone line. For example, the following steps show how to administer a softphone in telecommuter mode for a home user at extension 3010.

Procedure

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

   The system displays the Station screen.

   Note:

   For a new DCP extension, use the `add station` command. For an existing DCP extension, use the `change station` command, and ignore steps 3 and 4.
3. In the **Port** field, type `x` for virtual telephone, or enter the port number if there is hardware.
4. In the **Security Code** field, enter the password for this remote user.

   For example, enter `1234321`.

   This password can be up to 7 digits in length.
5. In the **IP Softphone** field, type `y`.
6. On page 2, in the **Service Link Mode** field, type `as-needed`.

   Set this field to permanent only for extremely busy remote telephone users, such as call center agents.
7. In the **Multimedia Mode** field, type `enhanced`.
8. Press `Enter` to save your work.

   Now you can install and configure the software on the user's Personal Computer. In this example, the user will login by entering their DCP extension (3010) and password (1234321).

Troubleshooting IP softphones

Problem

Display characters on the telephone cannot be recognized.

Cause

Microsoft Windows is not set to use Eurofont characters.

Solution

Set the Microsoft Windows operating system to use Eurofont.

For more information on how to install and configure the IP Softphone software, see user documentation on Avaya IP softphone.

Problem

The call is not connecting to the home phone that is configured as Other Phone.

Cause

The Facility Restriction Level (FRL) of the desk phone is too low for the route pattern over which the trunk call to the home phone is sent.

Solution

Increase the FRL of the desk phone or reduce the FRL on the route pattern.

IP Telephones

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.

Adding an IP telephone

Before you begin

Verify the system has a:

- TN2302 IP Media Processor circuit pack for audio capability
- TN799 Control-LAN circuit pack for signaling capability (for CSI Servers only)

Make sure that you can use IP Telephones on your system. Display the System-Parameters Customer-Options (Optional Features) screen, and verify the following field settings.

- **Maximum Concurrently Registered IP Stations** is greater than 0
- **IP Stations** field is y

- Information has been entered in the fields on the Maximum IP Registrations by Product ID page.

About this task

These steps show how to add an IP telephone at extension 4005 and how to assign an extension.

Procedure

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

   The system displays the Station screen.

   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 to access the Automatic Callback feature.

   The system displays the **Port** field as display only, and IP.
3. In the **Security Code** field, enter the password for the IP telephone user.

   Although the system accepts a null password, the IP telephone does not work unless you assign a password.
4. Press `Enter` to save your work.

Changing from dual-connect to single-connect IP telephones

About this task

When you have a dual extension telephone and you upgrade to a single extension telephone, you can remove the connection that is no longer used for that telephone. To remove the H.323 connection that is no longer needed, first record the media complex extension number.

Procedure

1. Type `change station nnnn` where nnnn is the extension number of the original dual-connect telephone that you are replacing with a single-connect telephone.

   The 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 work.
5. Remove the extension you recorded. Before you remove an H.323 extension from your system, check the status, remove it from any group or usage lists, and then delete it from the system's memory.

For example, if you wrote down extension 1234 before you removed it from the **Media Complex** field on the Station screen, then remove extension 1234 using these steps:

a. Type `status station 1234`.

b. Press `Enter`.

   The system displays the General Status screen.

c. Make sure that the extension is idle and not making or receiving calls, has no messages waiting and has no active buttons, such as **Send All Calls** or **Call Forwarding**.

d. Type `list groups-of-extension 1234`.

e. Press `Enter`.

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

f. Press `Cancel`.

g. If the extension belongs to a group, access the group screen and delete the extension from that group.

   If extension 1234 belongs to pickup group 2, type `change pickup group 2` and delete the extension from the list.

h. Type `list usage extension 1234`.

i. Press `Enter`.

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

j. Press `Cancel`.

k. If the system displays the extension on the Usage screen, access the appropriate feature screen and delete the extension.

   If extension 1234 belongs to hunt group 2, type `change hunt group 2` and delete the extension from the list.

l. Type `change station 1234`.

m. Press `Enter`.

n. Delete any bridged appearances or personal abbreviated dialing entries.

o. Press `Enter`.

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

p. Type `remove station 1234`.

q. Press `Enter`.

r. If this is the correct telephone, press `Enter`.
   - The system responds with `command successfully completed`.
   - If the system responds with an error message, the telephone is busy or still belongs to a group.

s. Press `Cancel` to stop the request, correct the problem, and type `remove station 1234` again.

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

u. Type `save translations`.

v. Press `Enter` to save your changes.

Note:

You do not need to delete the extension from coverage paths. The system automatically adjusts coverage paths to eliminate the extension.

Once you successfully remove the extension, it is permanently erased from system memory. If you want to reactivate the extension, you have to add it again as though it were new.

Setting up emergency calls on IP telephones

About this task

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

You use the Station screen to set up emergency call handling options for IP telephones. As an example, administer the option that prevents emergency calls from an IP telephone.

Procedure

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

   The system displays the Station screen.
3. Click `Next Page` to find the **Remote Softphone Emergency calls** field.
4. Type `block` in the **Remote Softphone Emergency calls** field.
5. Press `Enter` to save your changes.

Caution:

An Avaya IP endpoint can dial emergency calls, such as 911 in the U.S., but 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. 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. Go to the Avaya Support website at http://support.avaya.com if you have questions about emergency calls from IP telephones.

Remote office setup

Avaya Remote Office provides IP processing capabilities to traditional call handling for voice and data between Avaya Communication Manager and offices with Remote Office hardware. You need to add the information about Remote Office as a node in Communication Manager, add its extensions, and set up the trunk and signaling groups.

Adding Remote Office to Communication Manager

Before you begin

On the System Parameters Customer-Options (Optional Features) screen, ensure that the following fields are set to y.

- **Maximum Administered Remote Office Trunks**
- **Maximum Administered Remote Office Stations**
- **Product ID registration limit**
- **Remote Office**
- **IP station**
- **ISDN-PRI**

Also, install and administer your Remote Office hardware at the remote location and obtain the following information from the remote administration:

- IP address
- Password

About this task

As an example, set up a remote-office location using Avaya R300 Remote Office Communicator hardware, add a new node, and set up the signaling group and trunk group.

Procedure

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

   The system displays the Node Name screen.

3. In the **Name** field, type in a word to identify the node.

   Type `Remote 6`.

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

   The system displays the Remote Office screen.

8. Fill in the following fields.
   - **Node Name** - match the name on the IP Node Names screen.
   - **Network Region** - this must match the network region on the IP Interfaces screen for the circuit packs that connect this remote office. Use display ip-interfaces to find this information.
   - **Location** - match the one set up on the Location screen for this remote office.
   - **Site Data** - identify the street address or identifier you want to use.
9. Press `Enter` to save your changes.

Tip:

Use status remote office to verify that your server running Communication Manager recognizes the Remote Office information. It also displays the extensions and signaling group you administer next.

Setting up a trunk group

About this task

You can modify an existing trunk group or add a new one. In our example, we will add trunk group 6. Before you start, perform Setting up a signaling group on page 134.

Procedure

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 `H.323` (Medpro).
5. In the **Dial Access** field, type `y`.

6. In the **Service Type** field, type `tie`.
7. In the **Signaling Group** field, type in the signaling group you created.
8. Press `Enter` to save your changes.

Setting up a signaling group

About this task

Each Remote Office has its own listen port and signaling group. Set up a new trunk group, or use an existing trunk group administered for H.323 signaling. To set up the signaling group for remote office:

Procedure

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

   The 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 CLAN that supports the R300.
6. In the **Far-end Node Name** field, identify the node name assigned to the CLAN that supports the R300.
7. In the **Near-end Listen Port** field, type a port number in the 5000-9999 range.
8. In the **Far-end Listen Port** field, type `1720`.
9. In the **RRQ** field, type `y`.
10. Tab to the **Direct IP-IP Audio Connection** field on another page of this screen, and type `y`.
11. Press `Enter` to save your changes.

Setting up Remote Office on network regions

About this task

Now set up a network region to show the connections between regions. You can begin with network region 1.

Procedure

1. Type `change ip-network-region 1`.
2. Press `Enter`.

   The system displays the IP Network Region screen.

3. In the **Name** field, describe the region you are setting up.
4. In the **Stub Network Region** field, enter `y` if you are creating a stub network region or `n` if you are creating a core network region. For network regions 251 to 2000, this field is a read-only field and has a default value of `y`.

   If you are creating a stub network region, then on page 4, in the **dst rgn** field, you must enter the number of the destination core network region that this stub network region connects to.
5. In the **Codec Set** field, type the codec set you want to use in this region.
6. In the **UDP Port Range** field, type the range of the UDP port number to be used for audio transport.
7. In the **Intra-region IP-IP Direct Audio** field, type `y`.
8. In the **Inter-region IP-IP Direct Audio** field, type `y`.
9. Go to page 4 to set up connections between regions and assign codecs for inter-region connections.

   Page 3 of the IP Network Region screen shows a list of Survivable Remote Server for the network region.

   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
10. Assign the region number to the CLAN circuit pack. All the endpoints registered with a specific CLAN circuit pack belong to the CLAN region.

    For more information, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Adding telephones to Remote Office

Before you begin

Be sure the extensions you add fit your dialing plan.

Procedure

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

   The Station screen appears.
3. In the **Type** field, type in the model of the telephone you are adding.
4. In the **Port** field, type `x`.

   This indicates that there is no hardware associated with the port assignment.

5. In the **Name** field, identify the telephone for your records.
6. In the **Security Code** field, match the password set up on the Remote Office administration.
7. In the **Remote Office Phone** field, type `y`.
8. Press `Enter` to save your changes.

Downloading firmware to multiple stations

About this task

You can download firmware to multiple stations of the same type, either 2410, 2420, 1408, or 1416 DCP telephone. Download firmware to as many as 1000 stations per download schedule. You can schedule a specific time for the download, or you can administer the download to run immediately. To download 2410, 2420, 1408, or 1416 DCP station firmware to multiple stations:

Procedure

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

   The system displays the Firmware Station Download 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 start.
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 stop.
6. In the **Continue Daily Until Completed** field, enter `y` if you want the system to execute the firmware download each day at the scheduled time until all specified telephones have received the firmware.
7. In the **Beginning Station** field, enter the first extension number in the range of telephones to which you want to download the firmware.

   Up to 1000 stations can be included in a scheduled download.
8. In the **Ending Station** field, enter the last extension number in the range of telephones to which you want to download firmware.

   Up to 1000 stations can be included in a scheduled download.

   Note:

   Although you can specify a range of up to 1000 extensions, all 1000 stations are not downloaded simultaneously because there is a limit of how many concurrent telephones will be downloaded on a board, gateway, and port network. These limits will likely result in multiple "passes" required to attempt a download to the telephone.

Also note that on the first "pass", only two telephones will be attempted, and if multiple telephones fail, then the schedule may stop.

9. Press `Enter`.

   The firmware download is set to run at the scheduled time. If you entered `n` in the **Schedule Download?** field, pressing `Enter` immediately initiates the download to the specified range of telephones.

Displaying firmware download status

About this task

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

Procedure

1. Type `status firmware download`.

   The system displays the Status Firmware Station Download screen.

2. Press `Enter`.

Note:

If you add the qualifier last to the **`status firmware download`** command, status information on the last download schedule is displayed.

Disabling firmware downloads

About this task

To disable active downloads:

Procedure

Type `disable firmware download`.

This command disables any active download schedule, and the system displays

`Command successfully completed`

at the bottom of the screen.

Native Support of Avaya 1408 and 1416 digital telephones

Native support of Avaya 1408 (1400 Mid) and 1416 (1400 High) digital telephones is available from Communication Manager 6.0 and later. Communication Manager supports call processing features for the Avaya 14xx digital telephones just like Avaya 24xx digital telephones, along with support for the following:

- Fixed feature buttons (Hold, Conference, Transfer, Message waiting lamp, Drop and Redial)
- Message button

- 40 Unicode, Eurofont, or Kanafont character display message support
- Speakerphone functionality (including Group Listen)
- Eight call appearances or feature buttons

Note:

To allow firmware upgrades and to use the new capabilities of the sets, the telephone type must be administered as either 1408 or 1416 digital telephone.

Native Support of Avaya 1408 digital telephone

Communication Manager provides native administration for the Avaya 1408 digital telephone. The Avaya 1408 digital telephone administration is similar to the Avaya 2410 digital telephone with the same fields and default values except for the following:

- Support for eight call appearances or feature buttons
- No **Customizable Labels** field
- No **Media Complex Ext** field
- Support for display languages which include English, Spanish, French, Italian, User defined, Unicode, Unicode2, Unicode3, and Unicode4

Native Support of Avaya 1416 digital telephone

Communication Manager provides native administration for the Avaya 1416 digital telephone. The Avaya 1416 digital telephone administration is similar to the Avaya 2420 digital telephone with the same fields and default values except for the following:

- Support for 16 call appearances or feature buttons
- No **Customizable Labels** field
- No **Data Option** field
- No **Media Complex Ext** field
- Support for display languages which include English, Spanish, French, Italian, User defined, Unicode, Unicode2, Unicode3, and Unicode4
- Support for **Button Modules** field rather than **Expansion Module** field

BM32 Button Support

The Avaya 1416 digital telephone uses the BM32 button expansion module. Communication Manager supports two BM32 buttons for the Avaya 1416 digital telephone.

Native support for 96x1 H.323 and SIP deskphones

Communication Manager 6.2 and later provide native support for 96x1 H.323 and SIP deskphones. You can configure the sets as H.323 or SIP. Owing to the presence of Communication Manager, you can specify the station type as an H.323 set type that includes 9608, 9611, 9621, and 9641 or SIP type that includes 9608SIP, 9611SIP, 9621SIP, and 9641SIP. Communication Manager supports call processing features for Avaya 96x1 deskphones similar to the 96x1 H.323 or SIP 9630 deskphone.

For more information about the features of 96x1 H.323 and SIP deskphones, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Native support for Avaya J100 Series IP Phones

Communication Manager 8.0 and later provide support for Avaya J100 Series IP Phones. Avaya J100 Series IP Phones are SIP-based phones that provide enhanced user experience and superior call quality.

Communication Manager provides default endpoint templates corresponding to different models of Avaya J100 Series IP Phones. You can create and manage new station types of Avaya J100 Series IP Phones by using these templates.

For more information about the features of Avaya J100 Series IP Phones, see *Avaya Aura® Communication Manager Hardware Description and Reference* and *Avaya J100 Series IP Phones Overview and Specifications*.

Native support of Avaya 9404 and 9408 digital telephones

Native support of Avaya 9404 and 9408 digital telephones is available from Communication Manager 6.2 and later. Communication Manager supports call processing features for the Avaya 9404 and 9408 digital telephones are similar to the 24xx and 14xx line of DCP telephones, and supports languages in Unicode format. The Avaya 9404 and 9408 digital telephones have a look and feel similar to the 96x1 telephones. Standard Local Survivability (SLS) does not support 9404 and 9408 stations natively. You must administer 9404 and 9408 telephones as 24xx telephones to support SLS natively. Communication Manager also supports the following features for the Avaya 9404 and 9408 digital telephones.

- Fixed feature buttons (Hold, Conference, Transfer, Message waiting lamp, Drop and Redial)
- Message button
- Customized button labels
- 40 Unicode, Eurofont, or Kanafont character display message support
- Speakerphone functionality (including Group Listen)
- Support for the same set of Communication Manager call processing features that are supported by the 1416 telephone

Note:

You must administer the telephone type as either 9404 or 9408 to allow firmware upgrades and to use the new capabilities of the sets.

Native support of Avaya 9404 digital telephone

Communication Manager provides native administration for the Avaya 9404 digital telephone. The Avaya 9404 digital telephone administration is similar to the Avaya 2410 digital telephone with the same fields and default values except for the following:

- Support for display languages which include English, Spanish, French, Italian, User defined, Unicode, Unicode2, Unicode3, and Unicode4

Native support of Avaya 9408 digital telephone

Communication Manager provides native administration for the Avaya 9408 digital telephone. The Avaya 9408 digital telephone administration is similar to the Avaya 2420 digital telephone with the same fields and default values except for the following:

- Support for display languages which include English, Spanish, French, Italian, User defined, Unicode, Unicode2, Unicode3, and Unicode4.
- Support for **Button Modules** field rather than **Expansion Module** field.

BM12 Button Support

The Avaya 9408 digital telephone uses the BM12 button expansion module that supports 24 buttons per module. Communication Manager supports three BM12 buttons for the Avaya 9408 digital telephone.

Administer location per station

Use the Administer location per station feature to:

- Connect the IP telephones and softphones through a VPN to the branch that an employee is assigned to.
- Allow a VPN connected employee to have the same dialing experience as others in the office who are connected through a gateway.

Related links

[Preparing to administer location number on Station screen](#) on page 140
[Setting up location number on Station screen](#) on page 141

Preparing to administer location number on Station screen

Procedure

On the Optional Features screen, ensure that the **Multiple Locations** field is set to `y`. If this field is set to `n`, your system is disabled for the Administer location per station feature. Go to the Avaya Support website at http://support.avaya.com for assistance.

Note:

If the **Multiple Locations** field on the Optional Features screen is set to `n`, the **Location** field on the Station screen is hidden.

To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

Setting up location number on Station screen

Procedure

1. Enter `change station n`, where *n* is the extension number to which you want to assign a location.
2. In the **Location** field, enter a valid location number.

   This field appears only when the **Type** field is set to H.323 or SIP.
3. Select `Enter` to save your changes.

Note:

If the station extension is a SIP telephone type and if the application type is OPS on the Stations with Off-PBX Telephone Integration screen, then the Off-PBX screen's **Location** field is display-only and displays the value of the **Location** field of the corresponding Station screen.

Chapter 7: Telephone Features

Once you add a telephone to the system, you can use the Station screen to change the settings, such as adding or changing feature button assignments. You can assign features or functionality to each programmable button according to your choice. If you have 6400-series telephones, you can administer some of their own feature buttons. For more information, see *Setting up Terminal Self-Administration* for more information.

Note:

An NI-BRI telephone with Communication Manager has only the **Conference**, **Transfer**, **Hold**, and **Drop** feature buttons, none of which requires administration. On an NI-BRI telephone, you can assign additional feature buttons only as call appearances. As a result, NI-BRI telephone users must access all other features of Communication Manager using feature access codes. Additionally, the number of call appearance buttons administered in Communication Manager (the default is three) must match the number of call appearances programmed on the telephone. Finally, Communication Manager does not support bridged call appearances for NI-BRI telephones.

Adding feature buttons

Procedure

1. Type `change station nnnn` where nnnn is the extension for the telephone you want to modify.
2. Press `Enter`.
3. Press `Next Page` until you locate the **Button Assignment** section of the Station screen.

   Some telephones have several feature button groups. Make sure that you are changing the correct button. If you do not know which button on the telephone maps to which button-assignment field, see your telephone manual, or see *Telephone Reference*.
4. Enter the button name that corresponds to the feature you want to assign. To determine feature button names, press Help, or see *Telephone Feature Buttons Table*.

   Note:

   For certain newer telephones with expanded text label display capabilities, you can customize feature button labels to accept up to 13 alphanumeric characters. For more information about this feature, see *Increasing Text Fields for Feature Buttons*.

5. Press `Enter` to save your changes.

   Some telephones have default assignments for buttons. For example, the 8411D includes defaults for 12 softkey buttons. It already has assignments for features like Leave Word Calling and Call Forwarding. If you do not use an alias, you can easily assign different features to these buttons if you have different needs. If you use an alias, you must leave the default softkey button assignments. You can change the button assignments on the screen and the features work on the alias telephone, however the labels on the display do not change.

Related links

Increasing Text Fields for Feature Buttons on page 143
Telephone feature buttons table on page 145

Increasing Text Fields for Feature Buttons

If you are using certain newer telephones with expanded text label display capabilities, use the Increase Text Fields for Feature Buttons feature to program and store up to 13 character labels for associated feature buttons and call appearances. This feature is available for the following telephones:

- 2410 (Release 2 or newer)
- 2420 (Release 4 or newer)
- 4610 (IP Telephone Release 2.2 or later)
- 4620 (IP Telephone Release 2.2 or later)
- 4621 (IP Telephone Release 2.2 or later)
- 4622 (IP Telephone Release 2.2 or later)
- 4625 (IP Telephone Release 3.1 or later)

Related links

Telephone feature buttons table on page 145
Adding feature buttons on page 142

Enabling extended text fields for feature buttons

About this task

To enable extended text fields for feature buttons:

Procedure

1. Type `add station next` or `change station nnnn`, where nnnn is the extension of the telephone you want to customize feature button labels for.

The system displays the Station screen.

2. Ensure that **Customizable Labels** is set to `y`.

   This user uses this 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 the Adding Feature Buttons section.

   Note:

   You can also use the existing Abbreviated Dialing (AD) button type (Abr Program) to program AD labels. However, if you choose to use the Abr Program button to program AD labels, you are limited to 5 upper case characters. For more information on Abbreviated Dialing, see Adding Abbreviated Dialing Lists.

Restricting customization of feature button types

About this task

To manage the usage of your system's allocation of customized button labels to ensure that VIP users have the button label customization resource available to them, you can restrict button label customization of up to 50 specified button types for users who are not considered to be VIP users. To restrict customization of specific feature button types:

Procedure

1. Type `change button-restriction`.

   The system displays the Button Type Customization Restrictions screen.

2. Ensure that **Restrict Customization Of Button Types** is set to `y`.
3. In the fields under Restrict Customization Of Labels For The Following Button Types, enter the button type you want to restrict users from customizing.

   Note:

   When you enter the special button types abr-spchar or abrv-dial, the system displays an additional field 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 multi-appearance 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 require 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 must match the number of call appearances programmed on the telephone. By default, the number of call appearance buttons administered in Communication Manager is three.

Note that Communication Manager does not support bridged call appearances for NI-BRI telephones.

Table 2: Telephone Feature Buttons

Button name	Button label	Description	Maximum
#	AD	Autodial: Users can administer the hash (#) button as an autodial feature button by entering the Audix number in the **BUTTON ASSIGNMENTS** field on the Station screen.	1 per station
abr-prog	Abr Program	Abbreviated Dialing Program: Users can use this button to program abbreviated dialing and autodial buttons or to store or change numbers in a personal or group list associated with the station.	1 per station
abr-spchar	AbrvDial (char)	Abbreviated Dialing Special Character: You can use this button to enter an associated special character when programming. For example, the tilde (~), ~m (mark), the pause (~p), ~s (suppress), ~w (wait for dial tone), or ~W (wait forever)] .	1 each per station
abrdg-appr (Ext: ____)	(extension)	Bridged Appearance of an analog telephone: Users can use this button to have an appearance of a single-line telephone extension. Assign to a 2-lamp appearance button.	Depends on station type

Table continues…

Button name	Button label	Description	Maximum
abrv-dial (List: __ DC: __)	AD	Abbreviated Dialing: Users can use this button to dial the stored number on the specified abbreviated dialing list. List: Users can specify the list number 1 to 3 where the destination number is stored. DC: Users can specify the dial code for the destination number.	1 per AD list per dial code
abrv-ring	AbRng	Abbreviated and Delayed Ringing: Users can use this button to trigger an abbreviated or delayed transition for calls alerting at an extension.	
ac-alarm	AC Alarm	Administered Connection alarm notification: Users can use this button 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 : Users of display telephones can use this to identify trunk malfunctions. The system automatically initiates a referral call to the telephone when a possible failure occurs. When the user presses ACA Halt, the system turns off ACA monitoring for the entire system. The user must press ACA Halt again to restart monitoring.	1 per system
account	Account	Account: Using this button, the user can enter Call Detail Recording (CDR) account codes. With CDR account codes, the system can associate and track calls according to a particular project or account number.	1 per station
admin	Admin	Administration: With this button, a user can program the feature buttons on their 6400-series telephone.	1 per station
after-call Grp:___	AfterCall	After Call Work Mode: An agent can be temporarily removed from call distribution so that the agent can finish ACD-related activities, such as completing paperwork. Grp: Users can specify the ACD split group number.	1 per split group
agnt-login	Agent Login	Agent Login: This feature is used to log in an agent. Agent Login screen is displayed with Agent ID and password on the screen.	1 per station
alrt-agchg	Alert Agent	Alert Agent: This feature indicates to the agent that their split or skill hunt group changed while active on a call. This button blinks to notify the agent of the change.	1 per station

Table continues…

Button name	Button label	Description	Maximum
alt-frl	Alternate FRL	Alternate Facility Restriction Level (FRL): This feature activates or deactivates an alternate facility restriction level for the extension.	1 per system
ani-requst	ANI Request	Automatic Number Identification Request: Users can use this 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: An ACD agent can use this feature to place a call to a split supervisor. Group: You can specify the ACD split group number.	1 per split group
asvn-halt	ASVN Halt	Authorization Code Security Violation Notification: Activates or deactivates call referral when an authorization code security violation is detected.	1 per system
atd-qcalls	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 or deactivates recording of the current call. An Audix hunt group extension that is valid for the user must be entered in the Ext: field after the name.	1 per station
aut-msg-wt (Ext: ___)	Msg (name or ext #)	Automatic Message Waiting: Associated status lamp automatically lits 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 extension per button per phone
auto-cback	Auto CallBack	Automatic Call Back: Inside user can activate this to place 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

Table continues…

Button name	Button label	Description	Maximum
auto-in (Group: __)	Auto in	Auto-In Mode: With this the user can 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): Attendants, front-desk users, and guests can use this to request a wake up call to be placed automatically to a certain extension (cannot be a VDN extension) at a later time.	1 per station
autodial	SD	User can use this 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 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
brdg-appr	B	Use a numeric value from 1 to 32 to specify a tradition per-call appearance bridged appearance or use `a` to specify a multiple call arrangement bridged appearance.	
btn-ring	Button Ring	Station User Button Ring Control: Users can use this to toggle between audible and silent call alerting.	1 per station

Table continues…

Button name	Button label	Description	Maximum
btn-view	Button View	Button View: Users can use this 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. Users can use this 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 on behalf of the configured extension. If the extension is blank, the button applies to this station.	64 per extension
call-park	Call Park	Users can use this to place the current call in the call park state so it can be retrieved from another telephone.	1 per station
call-pkup	Call Pickup	Users can use this to answer a call that is ringing in the user's pickup group.	1 per station
call-timer	Call Timer	Used only on the 6400 sets. Users can use this to view the duration of the call associated with the active call appearance button.	1 per station
call-unpk	Unpark Call	Users can use this to unpark a call from another telephone than the telephone that originally parked the call. This feature button applies only to the SIP station types.	1 per station
callr-info	Caller Info	(Display button) Users can use Call Prompting to display information collected from the originator.	1 per station

Table continues…

Button name	Button label	Description	Maximum
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 (Ext: ___)	CFBDA (ext #)	Call Forward Busy or Don't Answer: Activates and deactivates call forwarding for calls when the configured extension is busy or the user does not answer. If the extension is blank, the button applies to this station.	64 per extension
cfwd-enh (Ext: ___)	ECFwd (ext #) Enhanced Cfwd (no ext #)	Users can use Call Forwarding-Enhanced to specify a different destination extension for both internal and external calls on behalf of the configured extension. If the extension is blank, the button applies to this station.	
check-in	Check In	Check In (display button): Changes the state of the associated guest room to occupied and turns off the outward calling restriction for the guest room's station.	1 per station
check-out	Check Out	Check Out (display button): Changes the state of the associated guest room to vacant and turns on the outward calling restriction for the guest room's station. Also clears (removes) any wake-up request for the station.	1 per station
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	Users can use this to display information about each party of a conference call. This button can be assigned to stations and attendant consoles.	1 per station

Table continues…

Button name	Button label	Description	Maximum
consult	Consult	The covering users uses the Consult button 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	A covering party uses this to store a leave word calling message for the principal (called party).	1 per station
cov-msg-rt	Covr Msg Ret	Coverage Message Retrieval (display button): Places a covering station into the message retrieval mode for the purposes of retrieving messages for the group.	1 per station
cpn-blk	CPN Block	Blocks the sending of the calling party number for a call.	1 per station
cpn-unblk	CPN Unblock	Deactivates calling party number (CPN) blocking and allows the CPN to be sent for a single call.	1 per station
crss-alert	Crisis Alert	Crisis Alert (display button): Provide this button to the telephones or consoles that you want to notify when any user makes an emergency call. (You define which calls are emergency calls on the AAR or 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): Using this DID assignments can be removed.	1 per station

Table continues…

Button name	Button label	Description	Maximum
did-view	DID View	DID View (display button): To display and change DID assignments and to choose between XDID and XDIDVIP numbers.	1 per station
directory	Directory	Directory (display button): Users with display telephone can 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. The users uses these buttons 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: Users uses this to answer a call ringing at another extension without having to be a member of a pickup group.	
disp-chrg	Disp Charges	Provides your display telephone with a visual display of accumulated charges on your current telephone call. Used exclusively outside the U.S. and Canada.	1 per station
disp-norm	Local/ Normal	Normal (display button): Toggles between LOCAL display mode (displays time and date) and NORMAL mode (displays call-related data). LED off = LOCAL mode and LED on = NORMAL.	1 per station
dn-dst	DoNotDisturb	Places the user in the do not disturb mode.	1 per station
drop	Drop	User can drop calls. Users can drop calls from automatic hold or drop the last party they added to a conference call.	

Table continues…

Button name	Button label	Description	Maximum
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: Multi-appearance telephone users can 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
ext-dn-dst	ExtDoNotDisturb	Extension — Do Not Disturb (display button): Used by the attendant console or hotel front desk display telephone to activate do not disturb and assign a corresponding deactivate time to an extension.	1 per station
ext-pkup	Call Pickup Extended	User uses this to answer calls directly from another call pickup group. This feature button applies only to the SIP station types.	1 per station
extnd-call	Extend Call	User uses this to extend the current call to an Off-PBX or EC500 telephone	1 per station
fe-mute	fe-mute Far End Mute	User uses this to mute a selected party on a conference call. This button can be assigned to stations and attendant consoles.	1 per station

Table continues…

Button name	Button label	Description	Maximum
flash	Flash	1. To allow a station on a trunk call with Trunk Flash to send a Trunk Flash signal to the far end (for example, Central Office). 2. To allow 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	Using this users can make announcements to groups of stations by automatically turning on their speakerphones. Number: The extension of the page group.	
headset	Headset	Signals onhook or 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
hntpos-bsy (Grp: ___)	Busy (Hunt Grp #)	Using this button, non-ACD hunt group users can opt-in or opt-out of hunt group calls.	1 per station per group
in-call-id (Type: __ Grp: ___)	INCallID (group #, type, name, or ext #)	A member of a coverage answer group or hunt group can use the Coverage Incoming Call Identification (ICI) button 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): Users use this on an active call to display the identification of an incoming call. Users can also use this to determine the identification of calls they placed on Hold.	1 per station

Table continues…

Button name	Button label	Description	Maximum
Inst-trans	Instant Transfer	An Instant Transfer button does an instant transfer by performing an immediate unsupervised transfer to the button's administered destination. The Instant Transfer button is intended for transfer to Polycom room systems, which are capable of hosting a conference and auto-answering calls as well. The Instant Transfer button is not limited to video set-types; however, it may be useful on other set-types as well.	1 per station
int-aut-an	IntAutoAnswer	Internal Automatic Answer: Causes any hybrid or digital station to automatically answer incoming internal calls.	1 per station
last-numb	LastNumb Dialed	Last Number Dialed (redial): Originates a call to the number last dialed by the station.	1 per station
lic-error	License Error	License-Error: Indicates a major License File alarm. Pressing the button does not make the light go out. The button goes out only after the error is cleared and Communication Manager returns to License-Normal Mode. You can administer this button on telephones and attendant consoles.	1 per telephone 20 per system (Server CSI)
limit-call	LimitInCalls	Limit Number of Concurrent Calls feature: Users can use this to limit the number of concurrent calls at a station to one call, where normally multiple call appearances can terminate at the station.	1 per station
link-alarm (link# ___)	Link Fail (link #)	Link Alarm: Associated status lamp indicates that a failure has occurred on one of the Processor Interface circuit pack data links. Link: Link number — 1 to 8 for multi-carrier cabinets or 1 to 4 for single-carrier cabinets.	8 per station
logout-ovr	Forced Logout Override	Overrides a forced logout by clock time.	1 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

Table continues…

Button name	Button label	Description	Maximum
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: A multi-appearance telephone user can use this to press a button on their telephone in order to light the Manual Message Waiting button at another telephone. You can administer this feature only to pairs of telephones, such as an assistant and an executive. For example, an assistant can press the man-msg-wt button to signal the executive that they have a call.	None
man-overid (TOD: _)	ManOverid	Immediate Manual Override (display button): The user (on a system with Time of Day Routing) can 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: User uses this to take control of a malicious call trace request. Once the user becomes the MCT controller, the system stops notifying other MCT control extensions of the MCT request. NOTE: To add an extension to the MCT control group, you must also add the extension on the Extensions Administered to have an MCT-Control Button screen. When the user presses the MCT Control button, the system first displays the called party information. Pressing the button again displays the rest of the trace information. The MCT controller must dial the MCT Deactivate feature access code to release control. Only H.323, DCP stations, and attendants can be an MCT Controller. The **mct-contr** button is not supported on any SIP endpoints.	1 per station
mf-da-intl	Directory Assistance	Multifrequency Operator International: User uses this to call Directory Assistance.	1 per station

Table continues…

Button name	Button label	Description	Maximum
mf-op-intl	CO attendant	Multifrequency Operator International: User uses this 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	Indicates 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 Personal Computer (headset or speakers or 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: Illuminates a message waiting lamp on an associated station.	1 per station
mwn-deact	MsgWaitDeact	Message Waiting Deactivation: Dims a message waiting lamp on an associated station.	1 per station
next	Next	Next (display button): Steps to the next message when the telephone’s display is in Message Retrieval or Coverage Message Retrieval mode. Shows the next name when the telephone’s display is in the Directory mode.	1 per station
night-serv	Night Service	Night Service Activation: Toggles the system in or out of Night Service mode.	1 per station
noans-alrt	NoAnsAlrt	Redirection on No Answer Alert: Indicates a Redirection on No Answer timeout has occurred for the split.	1 per hunt group
no-hld-cnf	No Hold Conf	No Hold Conference: Can automatically conference another party while continuing the existing call.	1 per station
normal	Normal	Normal (display button): Places the station’s display into normal call identification mode.	1 per station

Table continues…

Button name	Button label	Description	Maximum
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: User uses this 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: User uses this to display a specific message to callers.	1 per station
pr-awu-alm	pr-awu-alm AutoWakeAlarm	Automatic Wakeup Printer Alarm: Associated status lamp indicates that an automatic wake up 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: User uses this 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: User uses this 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

Table continues…

Button name	Button label	Description	Maximum
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
rs-alert	ResetAlert	The associated status lamp lights if a problem escalates beyond a warm start.	1 per station
rsvn-halt	RSVN Halt	Remote Access Barrier Code Security Violation Notification Call: Activates or deactivates call referral when a remote access barrier code security violation is detected.	1 per station
scroll	Scroll	Scroll (display button): User uses this 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 #)	Users use Send All Calls to temporarily direct all incoming calls for the configured extension to coverage regardless of the assigned call-coverage redirection criteria. Assign to a lamp button. If the extension is blank, the button applies to this station.	64 per extension
send-term	Send TEG	Send All Calls For Terminating Extension Group: User uses this 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

Table continues…

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: With this the user can use one button to manually signal the associated extension. The extension cannot be a VDN extension.	1 per signal extension

Table continues…

Button name	Button label	Description	Maximum
sip-sobsrv	Service Observing	This feature provides an opportunity for training and quality control in call centers. The observer connects to a call between an agent and a customer. Once an audio connection is established, the observer hears the conversation and can have the ability to talk. From Release 8.1.3 onwards, Communication Manager supports the **sip-sobsrv** button for J169 and J179 SIP stations. If the station type is J169 or J179, **Listen-Only** is the only button option available. For all CC station types such as J169CC and 9621SIPCC, **Listen-Only** and **Coach** button options are available. Following three modes can be used by the observer: • Listening mode: Here, the observer is only allowed to hear. Other participants (agent and customer) do not notice that their conversation is being monitored. • Talk mode: Here, the observer has bi-directional voice path. This mode is useful when the observer wants to join the conversation. All agents, customers, and observers hear each other. Talk and Coaching modes are useful for training. • Coach mode (CC stations only): Here, the observer can privately instruct the agent without the customer hearing the conversation.	1 per station
ssvn-halt	SSVN Halt	Toggle whether or not station security code violation referrals are made to the referral destination.	1 per station
sta-lock	Station Lock	When Station Lock is enabled, the only calls that can be made from the station are those allowed by the COR administered in the Station Lock COR field.	1 per station
start-bill	Start Bill	After an ACD agent answers a call, the agent can press this button to send an ISDN CONNECT message to the PSTN network to start the PSTN call–billing for a call at the PSTN switch.	1 per station
stored-num	Stored Number	Enables a display mode that displays the numbers stored in buttons.	1 per station
stroke-cnt (Code:_)	Stroke Count (#)	Automatic Call Distribution Stroke Count # (0, 1, 2, 3, 4, 5, 6, 7, 8, or 9) sends a message to CMS to increment a stroke count number.	Upto 10 per station

Table continues…

Button name	Button label	Description	Maximum
team	Team	The Team Button has two generic functions, a display function and an execution function. Using the display function any member of a team (monitoring station) can 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: The system displays this field when you enter the button type team. Enter the extension of the principal station of the virtual "team." Rg: The system displays 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 on the 6400 sets. With this the users can view the duration of the call associated with the active call appearance button	1 per station
togle-swap	Toggle-Swap	User can use this to toggle between two parties before completing a conference or a transfer	1 per station
trk-ac-alm	FTC Alarm	Facility Test Call Alarm: Associated status lamp lights when a successful Facility Test Call (FTC) occurs.	1 per station
trk-id	Trunk ID	Trunk Identification (display button): Identifies the tac (trunk access code) and trunk member number associated with a call.	1 per station
trunk-name	Trunk Name	(display button) Displays the name of the trunk as administered on the CAS Main or on a server without CAS.	1 per station
trunk-ns (Grp: ___)	Trunk NS	Trunk-Group Night Service: Places a trunk-group into night service. Grp: Trunk group number.	3 per trunk group
usr-addbsy	Add Busy Indicator	Adds the busy indicator.	1 per station
usr-rembsy	Remove Busy Indicator	Removes the busy indicator.	1 per station
uui-info	UUI-Info	Users can use this to see up to 32 bytes of ASAI-related UUI-IE data.	1 per station
verify	Verify	Busy Verification: User can use this to make test calls and verify a station or a trunk.	1 per station

Table continues…

Button name	Button label	Description	Maximum
vip-chkin	VIP Check In	VIP Check-in (display button): User can use this 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 wake up call and continues to flash until the call is answered. If the VIP wake up call is unanswered, the user can press the VIP Retry button to drop the call and reschedule the VIP wake up call as a classic wake up 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 wake up reminder call is generated. The user presses the button to place a priority (VIP) wake up call to a guest. To assign this button, you must have both Hospitality and VIP Wakeup enabled.	1 per station
voa-repeat	VOA Repeat	VDN of Origin Announcement. VDN of Origin Announcement must be enabled.	1 per station
voice-mail	Message	This is not an administrable button, but maps to the fixed hard "message" button on newer telephones.	1 per station
vu-display (format: __ ID: __)	Vu Display #	VuStats Display: The agent can use this to specify a display format for the statistics. If you assign a different VuStats display format to each button, the agent can use the buttons to access different statistics. You can assign this button only to display telephones. format: specify the number of the format you want the button to display ID (optional): specify a split number, trunk group number, agent extension, or VDN extension	limited to the number of feature buttons on the telephone
whisp-act	whisp-act WhisperAct	Whisper Page Activation: A user can use this 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 telephone must have a class of restriction (COR) feature using which the user can use whisper paging by intra switch calling.	1 per station
whisp-anbk	WhisperAnbk	Whisper Page Answerback: A user who received a whisper page can respond to the user who sent the page.	1 per station
whisp-off	WhisperOff	Deactivate Whisper Paging: Blocks other users from sending whisper pages to this telephone.	1 per station
work-code	Work Code	Call Work Code: An ACD agent can use this after pressing "work-code" to send up to 16 digits (using the dial pad) to CMS.	1 per station

Related links

Increasing Text Fields for Feature Buttons on page 143
Adding feature buttons on page 142

Abbreviated Dialing Lists

Abbreviated dialing is sometimes called speed dialing. You can use it 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. With this, you get access to selected numbers that some telephone users might otherwise be restricted from manually dialing. For example, a user might be restricted from making long-distance calls. However, you can program the number of a branch office that is long distance into an AD list as privileged. Then, the user can call this office location using AD, while still being restricted from making other long-distance calls.

Security alert:

Privileged group-number, system-number, and enhanced-number lists provide access to numbers that typically would be restricted.

Setting up a station to access a new group list

About this task

We will set up station 4567 so it has access to the new group list

Procedure

1. Type `change station 4567`.
2. Press `Enter`.
3. Press `Next Page` until you see Station screen (page 4), containing the **Abbreviated Dialing List** fields.
4. Type `group` in any of the **List** fields.
5. Press `Enter`.

   The system displays a blank **list number** field.
6. Type `3` in the **list number** field.

When you assign a group or personal list, you must also specify the personal list number or group list number.

7. Press `Enter` to save your changes.

   The user at extension 4567 can now use this list by dialing the feature access code for the list and the dial code for the number they want to dial. Alternatively, you can assign an abbreviated dialing button to this station using which the user can press one button to dial a specific stored number on one of their three assigned abbreviated lists.

Adding Abbreviated Dialing Lists

About this task

You can program a new group list.

Procedure

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

   The system displays the Abbreviated Dialing List screen. In our example, the next available group list is group 3.

3. Enter a number (in multiples of 5) in the **Size** field.

   This number defines the number of entries on your dialing list.

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

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

   If you want the user at 4567 to be able to change group list 3, enter `4567` in this field

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

   Each telephone number can be up to 24 digits long.

6. Press `Enter` to save your changes.

   You can display your new abbreviated-dialing list to verify that the information is correct or print a copy of the list for your paper records. Once you define a group list, you need to define which stations can use the list.

Troubleshooting abbreviated dialing lists

Dial list connects to wrong number

Problem

A user complains that using an abbreviated dial list dials the wrong number.

Possible Causes

- The user entered an wrong dial code.

- The dial code was wrongly defined.

Proposed solution

Procedure

1. Ask the user what number they dialed or button they pressed to determine which list and dial code they attempted to call.
2. Access the dialing list and verify that the number stored for the specific dial code corresponds to the number the user wanted to dial.

   To access a group list, type display abbreviated-dialing group x, press `Enter`, where x is a group list number
3. If the user dialed the wrong code, give them the correct code.
4. If the dial code is wrong, press `Cancel` and use the appropriate change command to re-access the abbreviated dialing list.
5. Correct the number.
6. Press `Enter`.

Cannot access dial list

Problem

A user cannot access a dial list

Possible Causes

- The specific list was not assigned to the user's telephone.
- The user dialed the wrong feature access code
- The user pressed the wrong feature button.
- The feature button was wrongly defined.

Proposed solution–Verify list assigned to telephone

Procedure

1. Type `display station nnnn`, where nnnn is the user's extension.
2. Press `Enter`.
3. Review the current settings of the **List1**, **List2**, and **List3** fields to determine if the list the user wants to access is assigned to their telephone.

Proposed solution–Verify feature access code

Procedure

1. Type `display feature-access-codes`.
2. Press `Enter`.
3. Verify that the user is dialing the appropriate feature access code.

Proposed solution–Verify feature button assignment

Procedure

1. Type `display station nnnn`, where nnnn is the user's extension.
2. Press `Enter`.
3. Review the current feature button assignments to determine whether:
   - The user was pressing the assigned button.
   - The list number and dial code are correct.

Abbreviated Dialing Lists-Limitations

There are limits to the total number of abbreviated dialing list entries, the number of personal dial lists, and the number of group dial lists that your system can store. Because of these limitations, you should avoid storing the same number in more than one list. Instead, assign commonly dialed numbers to the system list or to a group list. You can determine the abbreviated dialing storage capacity, by referring to the System Capacity screen for the abbreviated dialing values (type display capacity). For details on the System Capacity screen, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Bridged Call Appearances

The primary number of a telephone is the extension assigned to the telephone when the telephone is administered. On the Station screen, the **Extension** field displays the primary number of the telephone. On a multiappearance telephone, multiple appearances of this primary number can exist.

A bridged call appearance is an appearance of a primary number on a different telephone. In most ways, the bridged call appearance acts like the primary number appearance. For example, when someone calls an extension, you can answer the call at the primary telephone or at the bridged call appearances of that extension. When a call is received, the primary telephone and the bridged call appearances alert visually, with audible ringing as an administrable option. Likewise, a call that is made from a bridged call appearance carries the display information and the Class of Restriction (COR) of the primary number.

You can use a bridged call appearance to perform operations such as conference, transfer, hold, drop, and priority calling.

The enhanced Bridged Call Appearance feature is introduced for Communication Manager Release 6.3.2 and later. With this enhancement, Communication Manager matches the caller information on the bridged lines with the caller information on the principal stations.

The following table depicts the display on bridged call appearance for an incoming call when the enhanced Bridged Call Appearance feature is active.

	Calling party name is available	Calling party name is unavailable
Calling party number (CPN) is available	<calling name> <calling number>	CALL FROM <calling number>
Calling party number (CPN) is unavailable	<calling name>	<incoming trunk name> <incoming trunk access code>

Note:

SIP phones do not support the enhanced Bridged Call Appearance feature.

Related links

Enabling Enhanced Bridged Call Appearance on page 169

Setting Up Bridged Call Appearances

About this task

Create a bridged call appearance.

Procedure

1. Note the extension of the primary telephone.

   A call to this telephone lights the button and, if activated, rings at the bridged-to appearance on the secondary telephone.
2. If you want to use a new telephone for the bridged-to extension, duplicate a station.
3. Type `change station and the bridged-to extension`.
4. Press `Enter`.
5. Press `Next Page` until the system displays the **Feature Options** page of the Station screen.
6. For the **Per Button Ring Control** field (digital sets only):
   - If you want to assign ringing separately to each bridged appearance, type `y`.
   - If you want all bridged appearances to either ring or not ring, leave the default `n`.
7. Move to Bridge Call Alerting.
8. If you want the bridged appearance to ring when a call arrives at the primary telephone, type `y`. Otherwise, leave the default `n`.
9. Complete the appropriate field for your telephone type.
   - If your primary telephone is analog, move to the **Line Appearance** field and enter `abrdg-appr`
   - If your primary telephone is digital, move to the **BUTTON ASSIGNMENTS** field and enter `brdg-appr`.
10. Press `Enter`.

Btn and **Ext** fields appear. If **Per Button Ring Control** is set to y on the Station screen for the digital set, **Btn**, **Ext**, and **Ring** fields appear

11. Enter the primary telephone's button number that you want to assign as the bridged call appearance.

    This button flashes when a call arrives at the primary telephone.

12. Enter the primary telephone extension.
13. If the system displays the **Ring** field, one of the following can be set:
    - If you want the bridged appearance to ring when a call arrives at the primary telephone, type `y`.
    - If you do not want the bridged appearance to ring, leave the default `n`.
14. Press `Enter` to save your changes.
15. To see if an extension has any bridged call appearances assigned, type list bridge and the extension.
16. Press `Enter`.

    The user at extension 4567 can now use this list by dialing the feature access code for the list and the dial code for the number they want to dial. Alternatively, you can assign an abbreviated dialing button to this station using which the user can press one button to dial a specific stored number on one of their three assigned abbreviated lists.

Enabling Enhanced Bridged Call Appearance

About this task

For the caller information on bridged call appearances to be the same as the caller information on the principal station, perform the following task.

Note:

SIP phones do not support the enhanced Bridged Call Appearance feature.

Procedure

1. Type **`change cos`**.
2. On page 2 of the Class of Service screen, set the **Match BCA Display with Principal** field to `y`.

When to use Bridged Call Appearances

Following is a list of example situations where you might want to use bridged appearances.

- A secretary making or answering calls on an executive's primary extension: These calls can be placed on hold for later retrieval by the executive, or the executive can simply bridge onto the call. In all cases, the executive handles the call as if he or she had placed or answered the call. It is never necessary to transfer the call to the executive.

- Visitor telephones: An executive might have another telephone in their office that is to be used by visitors. It might be desirable that the visitor be able to bridge onto a call that is active on the executive's primary extension number. A bridged call appearance makes this possible.
- Service environments: It might be necessary that several people be able to handle calls to a particular extension number. For example, several users might be required to answer calls to a hot line number in addition to their normal functions. Each user might also be required to bridge onto existing hot line calls. A bridged call appearance provides this capability.
- A user frequently using telephones in different locations: A user might not spend all of their time in the same place. For this type of user, it is convenient to have their extension number bridged at several different telephones.

Extension to Cellular

Use the Extension to Cellular feature to extend your office calls and Communication Manager features to a cellular telephone. For a detailed description of the Extension to Cellular feature and how to administer it, see Extension to Cellular in *Avaya Aura® Communication Manager Feature Description and Implementation* or *Avaya Extension to Cellular User Guide*.

Extension to Cellular Setup Table

The following table provides a quick reference to the screens and fields used in administering the Extension to Cellular feature.

Table 3: Screens for administering Extension to Cellular

Screen Name	Purpose	Fields
Stations with Off-PBX Telephone Integration	Map station extensions to application types and	**All**
Off-PBX Telephone Mobile-Feature-Extension	Administer CTI feature.	**Mobile Call (CTI) Extension**
Feature Access Code (FAC)	Set up access codes for Communication Manager features.	**Feature Access Code**
Extension to Call Which Activate Features by Name	Map a dialed extension to activate a feature (FNE) within Communication Manager from a cell phone. Some FNEs require FAC administration.	**Extension**
Telecommuting Access	Create an Extension to Cellular remote access number.	**All**
Security-Related System Parameters	Define a system-wide station security code length.	**Minimum Station Security Code Length**

Table continues…

Screen Name	Purpose	Fields
Station	Assign feature buttons and timers. **Note:** Do not use station type XMOBILE. Endpoints configured as XMOBILE cannot access important enhancements to EC500, such as support for SIP trunk groups.	**BUTTON ASSIGNMENTS**
Language Translations	To review the office telephone feature button assignments	**All**
Numbering-Public/ Unknown Format	Assign 10-digit caller identification.	**All**
Coverage Path	Set up number of unanswered rings prior to coverage.	**Number of Rings**
Trunk Group	Enable Call Detail Recording for outgoing trunk.	**CDR Reports**
DS1 Circuit Pack	Administer a DS1 Circuit pack for R2MFC for EC500 use.	**Signaling Mode: CAS** **Interconnect: CO**
Trunk Group	Administer a trunk group for EC500 use. **Note:** For more information, see Extension to Cellular in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.	**Group Type** **Trunk Type** **Outgoing Dial Type** **Incoming Dial Type** **Receive Answer Supervision?**
Multifrequency-signaling- related-parameters	Administer MFC parameters needed for EC500. **Note:** For more information, see Guidelines for administering Multifrequency Signaling in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.	**Incoming Call Type: group-ii-mfc (for MFC signaling)** **Outgoing Call Type: group-ii-mfc (for MFC signaling)** **Request Incoming ANI (non-AR/ARS) y**
System Capacity	Verify used, available, and system station limits.	**Off-PBX Telephone - EC500** **Off-PBX Telephone - OPS** **Off-PBX Telephone - PBFMC** **Off-PBX Telephone - PVFMC**

Setting Up Extension To Cellular Feature Access Button

About this task

Extension to Cellular provides the capability to administer an Extension to Cellular feature access button on the user's office telephone to enable and disable the feature. You can also configure an optional timer. You administer this feature button on page 3 of the Station screen for the "host"

office extension to which Extension to Cellular is linked. The process described below explains how to administer an Extension to Cellular feature button and include the optional Extension to Cellular timer. The Extension to Cellular feature button is available on telephones which support administrable feature buttons.

Procedure

1. Type `change station n`, where n is the extension of an Extension to Cellular enabled station

   Type `1034`.

2. Press the `Next Page` button twice to display the Station screen (page 4).
3. Select an available feature button under the `BUTTON ASSIGNMENTS` header (button 4 was used in this example) and type `ec500` to administer an Extension to Cellular feature button on the office telephone.
4. Press `Enter`.

   Note:

   The **Timer** subfield displays, and defaults to n. Leaving the default setting of n excludes the timer state

5. Set the optional **Timer** subfield to `y` to include an Extension to Cellular timer state for the administered feature button

   When the timer state is included, the Extension to Cellular user can activate a one-hour timer to temporarily disable Extension to Cellular through this administered feature button.

6. Press **Enter**.

   The corresponding feature button on the office telephone is now administered for Extension to Cellular.

   Note:

   The feature status button on the office telephone indicates the current state of Extension to Cellular regardless of whether the feature was enabled remotely or directly from the office telephone.

   For additional information, see the *Avaya Extension to Cellular User's Guide, 210-100-700*.

Terminal Self-Administration

Before a user can enter the TSA Admin mode, their telephone must be completely idle. After a user presses the Admin button and enters a security code (if necessary), they are prompted, via the telephone's display, to choose features to administer to buttons on their telephone. The user can add, replace, or delete any of the following feature-button types from their telephone.

- CDR Account Code

- Automatic Dial
- Blank
- Call Forwarding
- Call Park
- Call Pickup
- Directed Call Pickup
- Group Page
- Send All Calls
- Toggle Swap
- Activate Whisper Page
- Answerback for Whisper Page
- Whisper Page Off

End-user button changes are recorded to the Communication Manager server's history log so that remote services can know what translations are changed.

Setting Up Terminal Self-Administration

Before you begin

To prevent users from changing another user's telephone administration, you can enable the system-wide option that requires users to enter a station security code before they can administer their telephone.

To enable this option:

1. Set the **Station Security Code for Terminal Self-Administration Required** on the Security-Related System Parameters screen to `y`.
2. If you enable this option, the user is prompted for the station security code when they press the **Admin** button. The user must enter the security code, followed by the pound (#) button or the **Done** softkey.

About this task

Users use Terminal self-administration (TSA) to administer some of their own feature buttons from their telephones. TSA is available for 6400-series, and 4612 and 4624 telephones. Users are prompted, via the telephone's display, to choose features to assign to buttons on their telephones.

You need to assign a security code to the user's Station screen for each user you want to enable access to TSA. You also need to assign the user an Admin feature button. For example, to assign a security code of 12345678 to extension 4234, complete the following steps:

Procedure

1. Type `change station 4234`,.
2. Press `Enter`.

   The system displays the Station screen for extension 4234.

3. In the **Security Code** field, type `12345678`

   You should assign unique security codes for each user. Once you enter the code and move off the field, the system changes the field to '*' for extra security.

4. In one of feature button fields, type `admin`.

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

5. Press `Enter` to save your changes.

Fixing Problems in Terminal Self-Administration

Symptom	Cause and Solution
When a telephone is in the Admin mode, the telephone is not able to accept any calls	The telephone is treated as if it were busy. Also, a user cannot make calls while in the Admin mode.
Any button state a telephone is in when the telephone enters the Admin mode stays active while the telephone is in the Admin mode.	
ACD agents who need access to the Admin mode of TSA must be logged off before pressing the Admin button.	If they are not logged off when they attempt to enter the Admin mode, they receive a denial (single-beep) tone.
Call Forwarding can be active and works correctly in the Admin mode.	An active **Call Forwarding** button cannot be removed when the telephone is in the Admin mode.
The telephone must be on-hook to go into the Admin mode.	The **Headset On/Off** button must be in the OFF position.
A telephone that is in the Admin mode of TSA cannot be remotely unmerged by the PSA feature.	If a user has Abbreviated and Delayed Ringing active, a call can be silently ringing at a telephone and the user might not realize it. This ringing prevents the user from entering the Admin mode of TSA.

Enterprise Mobility User

Enterprise Mobility User (EMU) is a software-only feature that provides the ability to associate the buttons and features of a primary telephone to a telephone of the same type anywhere within your company's enterprise.

A home station can be visited by another EMU user while the user is registered as an EMU visitor elsewhere. A home station can be used as a visited station while the principal user's EC500 or other Off-PBX applications are active. And the principal user can activate an Off-PBX application even if their home station is being visited by another EMU user.

Note:

In this document, any telephone that is not the primary telephone is referred to as the "visited" telephone and any server that is not the home server of the primary telephone is referred to as the "visited server."

System Requirements — EMU

The following is a list of requirements that you need for the EMU feature:

- QSIG must be the private networking protocol in the network of Communication Manager systems. This requirement also includes QSIG MWI

  Note:

  All systems in a QSIG network must be upgraded to Communication Manager 4.0 or later in order for the Enterprise Mobility User feature to function properly. If only some systems are upgraded, and their extensions expanded, the EMU feature might not work with the systems that have not been upgraded. Go to the AvayaSupport website at http://support.avaya.com for more information.

- Communication Manager Release 3.1 or later software must be running on the home server and all visited servers.
- All servers must be on a Linux platform. EMU is not supported on DEFINITY® servers.
- The visited telephone must be the same model type as the primary telephone to enable a optimal transfer of the image of the primary telephone. If the visited telephone is not the same model type, only the call appearance (**call-appr**) buttons and the message waiting light are transferred.
- All endpoints must be terminals capable of paperless button label display.
- Uniform Dial Plan (UDP)
- To activate the EMU feature, a user enters the EMU activation feature access code (FAC), the extension number of their primary telephone, and the security code of the primary telephone on the dial pad of a visited telephone. The visited server sends the extension number, the security code, and the set type of the visited telephone to the home server. When the home server receives the information, it:
  - Checks the class of service (COS) for the primary telephone to see if it has PSA permission
  - Compares the security code with the security code on the Station screen for the primary telephone

- Compares the station type of the visited telephone to the station type of the primary telephone. If both the visited telephone and the primary telephone are of the same type, the home server sends the applicable button appearances to the visited server. If a previous registration exists on the primary telephone, the new registration is accepted and the old registration is deactivated

If the registration is successful, the visited telephone assumes the primary telephone's extension number and some specific administered button types. The display on the primary telephone shows **Visited Registration Active: <Extension>:** The extension number that displays is the extension number of the visited telephone

Note:

The speed dialing list that is stored on the primary telephone and the station logs are not downloaded to the visited telephone.

Configuring your System for the Enterprise Mobility User

Procedure

1. Type `display cos` to view your Class of Service settings.

   The system displays the Class of Service screen.

2. Verify that the **Personal Station Access (PSA)** field is set to `y`.

   This field applies to the primary telephone and must be set to y for EMU.

3. Type `display feature-access-codes`.

   The system displays the Feature Access Code (FAC) screen

4. In one of feature button fields, type `admin`.

5. Scroll down until you see the fields for **Enterprise Mobility User Activation and Deactivation**.

   The feature access codes (FACs) for both EMU activation and EMU deactivation must be set on all servers using EMU. You must enter the FAC of the server in the location from which you are dialing.

   Note:

   To avoid confusion, Avaya recommends that all the servers in the network have the same EMU feature access codes.

6. On page 3 of the Feature Related System Parameters screen, use the **EMU Inactivity Interval for Deactivation** (hours) field to administer a system-wide administrable interval for EMU deregistration at a visited switch.

7. Click `Enter` to save your changes.

Setting EMU options for stations

Procedure

1. Enter `add station next`.
2. Enter the security code of your primary telephone when you activate or deactivate EMU. The security code is administered on page one of the Station screen. The security code can be up to eight numbers. No letters or special characters are allowed. Once the security code is entered, the system displays a * in the **Security Code** field.
3. On the Station screen, scroll down till you find the **EMU Login Allowed** field.

   The **EMU Login Allowed** field applies to the visited station and must be set to y for EMU. The valid entries to this field are y or n, with n as the default. You must set this field to `y` to allow this telephone to be used as a visited station by an EMU user.
4. Select `Enter` to save your changes.

Defining options for calling party identification

Procedure

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

   The system displays the Trunk Group screen.
2. Scroll down till you see the **Send EMU Visitor CPN** field.

   This field controls calling party identification, that is, the extension of the primary telephone or the extension of the visited telephone that is used when a call is made from a visited telephone.
3. If you want the system to display calling party information of the primary telephone, the **Send EMU Visitor CPN** field must be set to `y`. There are areas where public network trunks disallow a call if the calling party information is invalid. In this case, there can be instances where the extension of the primary telephone is considered invalid and the extension of the visited telephone must be used. To use the extension of the visited telephone, set the **Send EMU Visitor CPN** field to `n`.

   Note:

   If you set the **Send EMU Visitor CPN** field to `y`, you must set the **Format** field on the same page to either public or unk-pvt.
4. Click `Enter` to save your changes.

Activating EMU

Procedure

1. At the visited telephone, enter the EMU activation Feature Access Code (FAC).

   You must enter the EMU activation FAC of the server in the location where you are dialing from.

2. Enter the extension of your primary telephone set.
3. Enter the security access code of your primary telephone set. This is the security code administered on the primary telephone's station form on the home server.
   - If the registration is successful, you hear confirmation tone.
   - If the registration is unsuccessful, you hear audible intercept.

   Audible intercept is provided when:
   - The registration was rejected by the home server.
   - The telephone where the registration attempt is made is not administered for EMU use.
   - The 15 second timer expires at the visited server.

   If the home server receives a request from a visited server for a telephone that already has an EMU visitor registration active, the old registration is terminated and the new registration is approved. If the primary telephone is in-use when a registration attempt is made, the registration attempt fails.

Deactivating EMU

Procedure

1. At the visited telephone, enter the EMU deactivation FAC.

   You must enter the EMU deactivation FAC of the server in the location where you are dialing from.
2. Enter the extension number of the primary telephone.
3. Enter the security code of the visited telephone.

   If the visited telephone does not deactivate, the telephone remains in the visited state.
4. To deactivate the visited telephone you can perform a busy-out, release busy-out at the visited server.
5. Enter the EMU feature deactivation code and the security code of the visited telephone at the home server location.
6. Press the `<mute>RESET` function on the IP telephone.

   Note:

   Anytime the visited telephone performs a reset, the EMU registration is deactivated.
7. Unplug the visited DCP set for a period of one minute

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

Chapter 8: Managing Attendant Consoles

Attendant Consoles

The attendant console is the main answering position for your organization. The console operator is responsible for answering incoming calls and for efficiently directing or "extending" calls to the appropriate telephone. Using the attendant console your attendants can monitor:

- system problems
- toll fraud abuse
- traffic patterns

The number of consoles you can have in your organization varies depending on your Avaya solution.

302 attendant consoles

Avaya Communication Manager supports the following 302 attendant consoles: the 302A/B, 302C, and 302D consoles. You might have a basic or enhanced version of these consoles.

To compare and contrast the consoles, view the diagrams below.

- 302A/B
- 302C
- 302D

302D Console

The 302D console provides the following enhancements to the 302C console:

- Modular handset or headset connection

  The console accepts a standard RJ11, 4-pin modular handset or headset. This connection replaces the quarter-inch, dual-prong handset or headset connection.

- Activate or deactivate push-button

  You can use the push-button on the left side of the console to activate or deactivate the console. The system displays a message on the console identifying that the button must be pressed to activate the console.

- Two-wire DCP compatibility

  The console is compatible with two-wire DCP circuit packs only, not four-wire DCP circuit packs.

- Headset volume control

The console can now control the volume of an attached headset.

- Noise expander option

  The console has circuitry to help reduce background noise during pauses in speech from the console end of a conversation. This option is normally enabled.

- Support for Eurofont or Katakana character set

  The console can show the Eurofont or Katakana character set. Administration of these character sets must be coordinated with the characters sent from Avaya Communication Manager.

Avaya Personal Computer consoles

The Avaya Personal Computer Console is a Microsoft Windows-based call handling application for Avaya Communication Manager attendants. It provides an ideal way to increase your productivity and to serve your customers.

Personal Computer 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.

Personal Computer 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 Personal Computer Console resides on a Windows-based Personal Computer, 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 Personal Computer Console, go to the Avaya Support website at http://support.avaya.com.

SoftConsole IP Attendant

The SoftConsole is a Windows-based application that can replace the 302B hard console. The SoftConsole is similar to Personal Computer Console, but it performs call answering and routing through a Personal Computer interface via IP. For more information, go to the Avaya Support website at http://support.avaya.com.

Related links

302A/B Console on page 181
302C Console on page 182
302D Console on page 183

302A/B Console

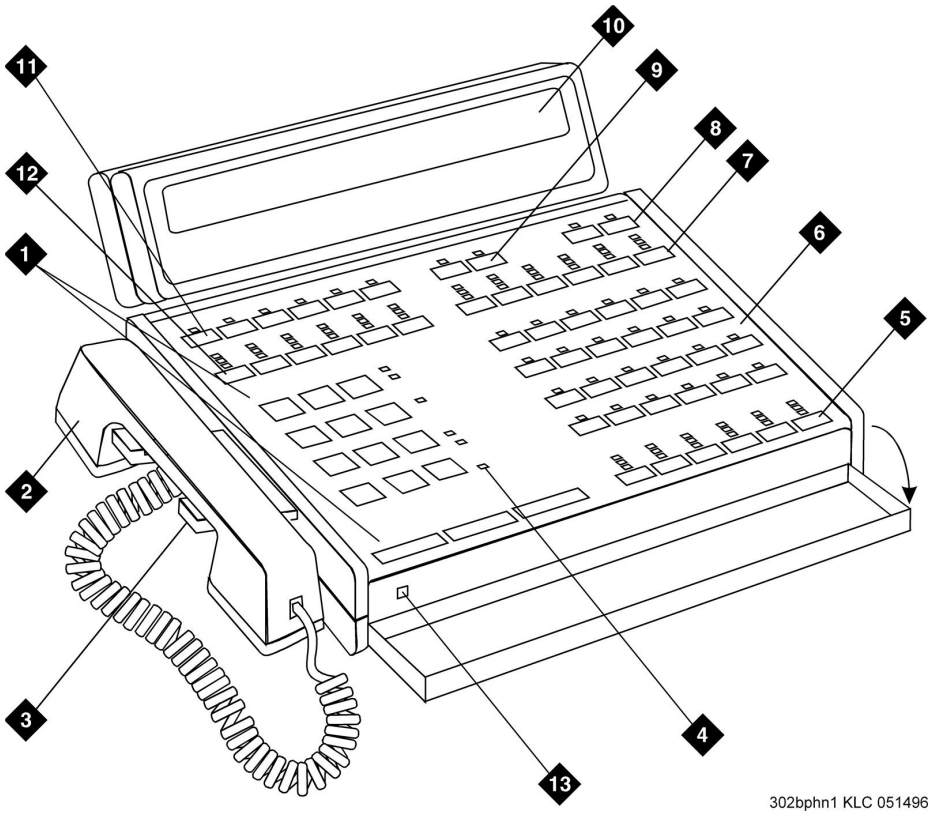


Figure 7: 302A and 302B1 attendant console

Note:

Button numbers map to physical positions on the console.

Figure notes:

1. Call processing area
2. Handset
3. Handset cradle
4. Warning lamps and call waiting lamps
5. Call appearance buttons
6. Feature area
7. Trunk group select buttons
8. Volume control buttons
9. Select buttons
10. Console display panel
11. Display buttons

12. Trunk group select buttons
13. Lamp Test Switch

Related links

Attendant Consoles on page 179

302C Console

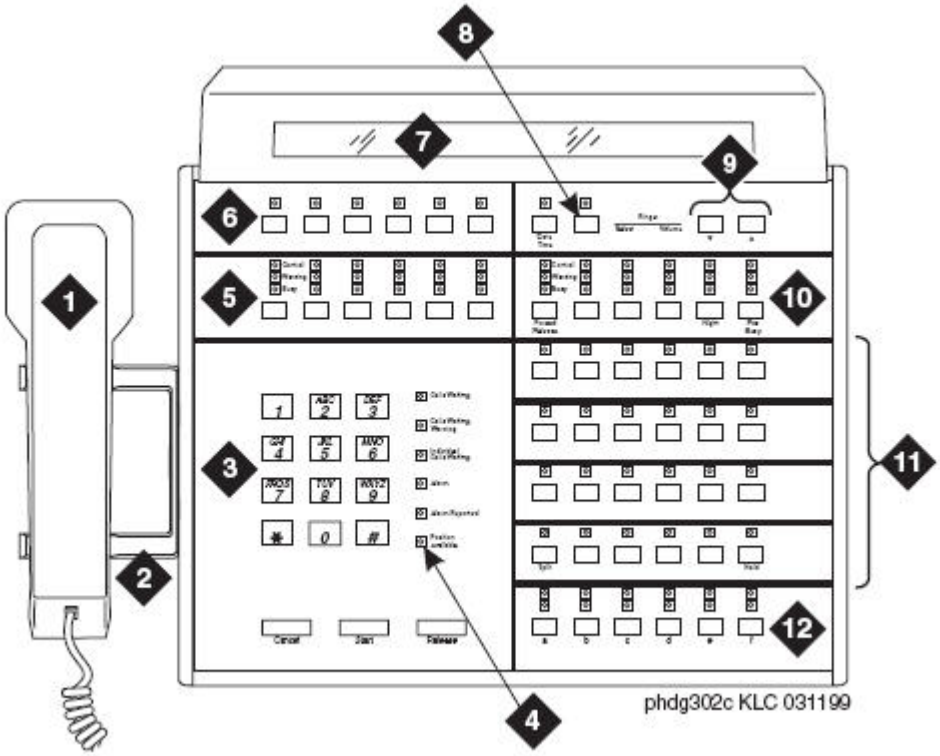


Figure 8: 302C attendant console

Note:

Button numbers map to physical positions on the console.

Figure notes:

1. Handset
2. Handset cradle
3. Call processing area
4. Warning lamps and call waiting lamps
5. Outside-line buttons
6. Display buttons
7. Display

8. Select buttons
9. Volume control buttons
10. Outside-line buttons
11. Feature buttons
12. Call appearance buttons

Related links

Attendant Consoles on page 179

302D Console

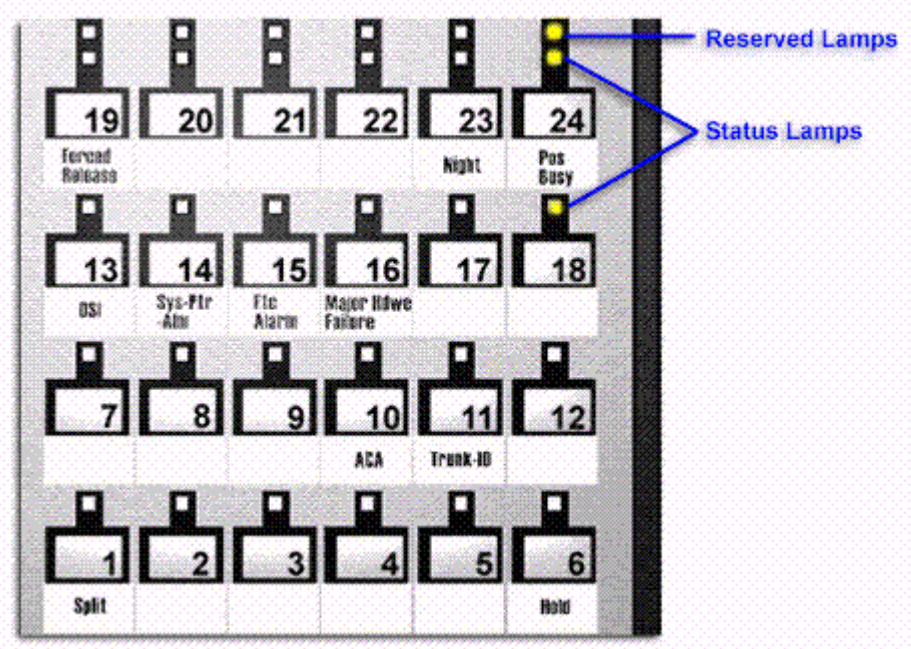


Figure 9: Console feature button layout

Note:

Button numbers map to physical positions on the console.

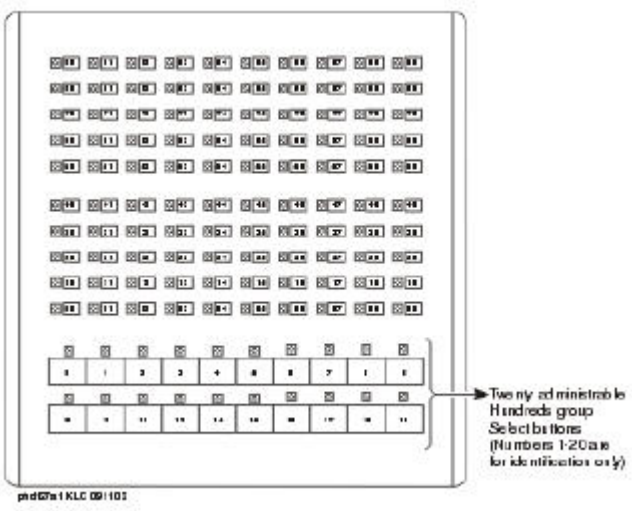


Figure 10: Enhanced Selector Console

Related links

[Attendant Consoles](#) on page 179

Adding an Attendant Console

About this task

Usually Avaya connects and administers your primary attendant console during cutover. However, you might find a need for a second attendant console, such as a backup console that is used only at night. This example shows how to add a night-only attendant console.

Note:

These instructions do not apply to adding a Personal Computer Console or SoftConsole. For more information, see the appropriate console documentation.

Procedure

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

   The system displays the Attendant Console 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.

Attendants can use Individual attendant extensions to use features that an attendant group cannot use — for example, you can assign them to hunt groups.

5. In the **Console Type** field, enter `night-only`.

   This indicates how this console is used in your organization—as a principal, day only, night only, or day/night console. You can have only one night-time console (night only or day/night) in the system.

6. In the **Port** field, enter the port address for this console.
7. Type a name to associate with this console in the **Name** field.
8. In the **DIRECT TRUNK GROUP SELECT BUTTON ASSIGNMENTS** fields, enter trunk access codes for the trunks you want the attendant to be able to select with just one button.
9. If you are using the **Enhanced Selector** console, set the **HUNDREDS SELECT BUTTON ASSIGNMENTS** that you want this console to have.

   If you want this console to be able to access extensions in the range 3500 to 3999, you need to assign them 5 **Hundreds Select Buttons**: 35 for extensions 3500 to 3599, 36, 37, 38, and 39.

10. Assign the Feature Buttons that you want the 302 console to have.

    To determine which buttons you can assign to a console, see *Attendant Console Feature Buttons*.

    Tip:

    Feature buttons are not numbered top-to-bottom on the attendant console, as you might expect.

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

Related links

Attendant Console Feature Buttons on page 185

Attendant Console Feature Buttons

Feature Buttons

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

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	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
	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
Attendant Override	Override	override	1	

Table continues…

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
Automatic Circuit Assurance	ACA	aca-halt	1 per system	
Automatic Wakeup (Hospitality)	Auto Wakeup	auto-wkup	1	
Busy Verification	Busy Verify	verify	1	
Call Coverage	Cover Cback	cov-cback	1	
	Consult	consult	1	
	Go To Cover	goto-cover	1	
Call Coverage [display button]	Cover Msg Rt	cov-msg-rt	1	
Call Offer (Intrusion)	Intrusion	intrusion	1	
Call Prompting [display button]	Caller Info	callr-info	1	
Call Type	Call Type	type-disp	1	
Centralized Attendant Service	CAS-Backup	cas-backup	1	
Check In/Out (Hospitality) [display buttons]	Check In	check-in	1	
	Check Out	check-out	1	
Class of Restriction [display button]	COR	class-rstr	1	
Conference Display [display button]	Conference Display	conf-dsp	1	
Demand Print	Print Msgs	print-msgs	1	
DID View	DID View	did-view	1	
Do Not Disturb (Hospitality)	Do Not Disturb	dn-dst	1	
Do Not Disturb (Hospitality) [display buttons]	Do Not Disturb Ext	ext-dn-dst	1	
	Do Not Disturb Grp	grp-dn-dst	1	
Don’t Split	Don’t Split	dont-split	1	
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	

Table continues…

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
Far End Mute [display button]	Far End Mute for Conf	fe-mute	1	
Group Display	Group Display	group-disp	1	
Group Select	Group Select	group-sel	1	
Hardware Failure [status lamps]	Major Hdwe Failure	major-alrm	10 per system	
	Auto Wakeup	pr-awu-alm	1	
	DS1 (facility)	ds1-alarm	10 per system	
	PMS Failure	pms-alarm	1	
	PMS Ptr Alm	pr-pms-alm	1	
	CDR 1 Failure	cdr1-alrm	1	
	CDR 2 Failure	cdr2-alrm	1	
	Sys Ptr Alm	pr-sys-alm	1	
Hold	Hold	hold	1	
Integrated Directory [display button]	Integrtd Directory	directory	1	
Incoming Call Identification	Coverage (Group number, type, name, or ext.#)	in-call-id	N	
Intrusion (Call Offer)	Intrusion	intrusion	1	
Leave Word Calling	Cancel LWC	lwc-cancel	1	
	LWC	lwc-store	1	
Leave Word Calling [display buttons]	Delete Msg	delete-msg	1	
	Next	next	1	
	Call Display	call-disp	1	
Leave Word Calling (Remote Message 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	

Table continues…

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
Off Board Alarm	off-bd-alm	off-bd-alm	1 per group	
Page 1 Link Alarm Indication	PAGE1 Alarm	pg1-alarm	1 per station	
Page 2 Link Alarm Indication	PAGE2 Alarm	pg2-alarm	1 per station	
PMS Interface [display buttons]	PMS display			
Priority Attendant Group	prio-grp	prio-grp	1	
Priority Calling	Prior Call	priority	N	
Position Busy	Position Busy	pos-busy	1	
Queue Status Indications (ACD) [display buttons]	AQC	atd-qcalls	1	
	AQT	atd-qtime		
Queue Status Indications (ACD) [status lamps]	NQC	q-calls (Grp:_)	1	10
	OQT	q-time Grp:_)	1 per hunt group	10
Remote Access Security Violation	rsvn-halt	rsvn-halt	1 per system	
Ringing	In Aud Off	in-ringoff	1	
Security Violation Notification Halt	ssvn-halt	ssvn-halt	1 per system	
Serial Call	Serial Call	serial-cal	1	
Split/Swap	Split-swap	split-swap	1	11
System Reset Alert	System Reset Alert [status lamp]	rs-alert	1	
Station Security Code Notification Halt	ssvn-halt	ssvn-halt	1 per system	
Night Service (ACD)	Hunt Group	hunt-ns (Grp. No.__)	3 per hunt group	12
Time of Day Routing [display buttons]	Immediate Override	man-ovrid	1	
	Clocked Override	clk-overid	1	
Timed Reminder	RC Aud Off	re-ringoff	1	
Timer	Timer	timer	1	
Trunk Identification [display button]	Trunk-ID	trk-id	1	
Trunk Group Name [display button]	Trunk-Name	trunk-name	1	

Table continues…

Feature or Function	Recommended Button Label	Value Entered on Attendant Console Screen	Maximum Allowed	Notes
Visually Impaired Service (VIAS)	VIS	vis	1	
	Console Status	con-stat	1	
	Display	display	1	
	DTGS Status	dtgs-stat	1	
	Last Message	last-mess	1	
	Last Operation	last-op	1	
VDN of Origin Announcement Repeat	VOA Repeat	voa-repeat	1	12
VuStats	VuStats	vu-display	1	

1. List: List number 1 to 3 where the destination number is stored. DC: Dial codes of destination number.
2. Grp: The split group number for ACD.
3. Code: Enter a stroke code (0 through 9).
4. TAC: local-tgs — TAC of local TG

   remote-tgs — (L-TAC) TAC of TG to remote PBX

   remote-tgs — (R-TAC) TAC of TG on remote PBX

   The combination of local-tgs/remote-tgs per console must not exceed 12 (maximum). Label associated button appropriately so as to easily identify the trunk group.
5. Grp: Enter a hundreds group number (1 through 20).
6. **Enhanced Hospitality** must be enabled on the System-Parameters Customer-Options (Optional Features) screen.
7. Ext: Can be a VDN extension.
8. Link: A link number — 1 to 8 for multi-carrier cabinets, 1 to 4 for single-carrier cabinets.
9. Grp: A trunk group number.
10. Grp: Group number of the hunt group.
11. The attendant can alternate between active and split calls.
12. VDN of Origin must be enabled.

Setting Console Parameters

About this task

You can define system-wide console settings on the Console Parameters screen. For example, if you want to warn your attendants when there are more than 3 calls in queue or if a call waits for more than 20 seconds, complete the following steps:

Procedure

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

   The system displays the Console Parameters screen.
3. In the **Calls in Queue Warning** field, enter `3`.

   The system lights the console's second call waiting lamp if the number of calls waiting in the attendant queue exceeds 3 calls. Click **Next** to display page 2.
4. In the **Time in Queue Warning** field, enter `20`.

   The system issues a reminder tone if a call waits in the attendant queue for more than 20 seconds.
5. Press `Enter` to save changes.

   Note:

   Some of the settings on the individual Attendant Console screens can override your system-wide settings.

Removing an Attendant Console

About this task

This procedure describes how to remove an attendant from the system. In this example, attendant 3 is assigned to extension 4345.

Procedure

1. Type `status attendant 3` and press **Enter**.

   The system displays the Attendant Status screen.
2. Make sure that the attendant console is plugged into the jack and is idle, not making or receiving any calls.
3. Type `list usage extension 4345` and press **Enter**.

   The Usage screen displays the usage of the extension in the system.
4. If the system displays the attendant extension on the Usage screen, press **Cancel**, access the appropriate feature screen and delete the extension.

   For example, if extension 4345 belongs to hunt group 2, type `change hunt group 2` and delete the extension from the list.
5. Type `remove attendant 3` and press **Enter**.

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

6. If the attendant that you have chosen is the correct attendant, save the changes.

   If the system displays an error message that the attendant group must be taken out of night service before removal or change, deactivate the Night Service feature.

7. If the extension has a voice mailbox, remove the extension from voice mail service.
8. Type `save translations` and press **Enter**.
9. Unplug the console from the jack and store it for future use.

   Note:

   You do not need to:

   - Delete the extension from the coverage paths. The system automatically adjusts coverage paths to eliminate the extension.
   - Disconnect the wiring at the cross-connect field.

   Note:

   The extension and port address remain available for assignment at a later date.

Providing Backup for an Attendant

Before you begin

- You can assign the attendant backup alerting only to multiappearance telephones that have a client room class of service (COS) set to No. For more information, see *Class of Service*.
- If you have not yet defined a Trunk Answer Any Station (TAAS) feature access code, you need to define one and provide the feature access code to each of the attendant backup users. For more information, see *Feature Access Code (FAC)*.

To enable your system to alert backup stations, you need to administer the Console Parameters screen for backup alerting. You also need to give the backup telephones an attendant queue calls feature button and train your backup users how to answer the attendant calls.

About this task

You can configure your system using Communication Manager so that you have backup positions for your attendant. Attendant Backup Alerting notifies backup telephones that the attendant need assistance in handling calls. The backup telephones are alerted when the attendant queue reaches the queue warning level or when the console is in night service.

Once a backup telephone receives an alert, the user can dial the Trunk Answer Any Station (TAAS) feature access code (FAC) to answer the alerting attendant calls.

Tip:

You can find more information about attendant backup in the *GuestWorks Technician Handbook*.

Procedure

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

   The system displays the Console Parameters screen.
3. In the **Backup Alerting** field, enter `y`.
4. Press `Enter` to save changes.

   The system will now notify anyone with an attendant queue calls button when the attendant queue reaches the warning level or when the console is in night service.
5. Type `change station 4345`.
6. Press `Enter`.

   The system displays the Station screen.
7. In one of the Button Assignment fields, enter `atd-qcalls`.

   The atd-qcalls button provides the visual alerting for this telephone. When this button is dark (idle state), there are no calls in the attendant queue. When the button shows a steady light (busy state), there are calls in the attendant queue. When button shows a flashing light (warning state), the number of calls in the attendant queue exceeds the queue warning. The backup-telephone user also hears an alerting signal every 10 seconds.
8. Press `Enter` to save changes.

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

Chapter 9: Managing Telephone Displays

Displaying administration

This chapter provides information about 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 active on a call. The information is displayed for 30 seconds on all telephones except Call Master telephones. The display goes blank after 30 seconds on Call Master telephones. However the information for each new call overrides the existing message.

The system displays the call information on the display only if the call terminates at the telephone. For example, if the call is forwarded to another extension, the system does not display the call information.

See the Telephone Displays feature description in the *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-505.

Displaying ANI Calling Party Information

About this task

Calling party information might consist of either a billing number that sometimes is referred to as Automatic Number Identification (ANI), or a calling party number. Your telephone might display the calling party number and name, or the incoming trunk group name.

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

Procedure

1. Type `change trunk group nnnn`, where nnnn is the trunk group you want to change.
2. Click **Next Page** until you see the **Trunk Parameters** fields on the Trunk Group screen (page 2).
3. Type `tone` in the **Incoming Dial Type** field.
4. Click **Next Page** and type `*ANI*DNIS` in the **Incoming Tone (DTMF) ANI** field.
5. Press `Enter` to save your changes.

Displaying ICLID Information

Before you begin

Be sure the **Analog Trunk Incoming Call ID** field is set to y on the System-Parameters Customer-Options (Optional Features) screen. See the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207 for information on the required circuit pack.

About this task

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

This example shows how to set up the analog diod trunk group 1 to receive calling party information and display the calling party number on the telephone of the person called.

Procedure

1. Type `change trunk group 1`.

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

Setting the Display Language

Procedure

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

   The System displays the Station screen.
3. In the **Display Language** field, enter the display language you want to use.

   Tip:

   Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except english, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.).To display time in 24-hour format and display messages in English, set the **Display Language** field to `unicode`. When you enter unicode, the station displays time in 24-hour format,

and if no Unicode file is installed, displays messages in English by default. For more information on Unicode, see *Administering Unicode display*.

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

Related links

Administering Unicode Display on page 196

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 Phone Message files avaya_unicode.txt and custom_unicode.txt, you must have Unicode-capable stations, such as the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones, and Avaya Softphone R5.0. Unicode is also an option for the 2420J telephone when **Display Character Set** on the System Parameters Country-Options screen is katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide*, 555-250-701.

Only Unicode-capable stations have the script (font) support that is required to match the scripts that the Unicode Phone Message file uses. To use the user-defined messages files avaya_user-defined.txt and custom_user-defined.txt you must use an Avaya digital 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 Phone Message Files

About this task

A Unicode Message file for each supported language is available in a downloadable ZIP file on the Avaya support Web site (https://support.avaya.com/unicode). You can also create a new translation or edit an existing translation with the Avaya Message Editing Tool (AMET) (https://support.avaya.com/amet). Additional languages are periodically becoming available, so check this site often for the most up-to-date message files.

Note:

Refer to the *Communication Manager Messages Job Aid* for details on the following procedures.

Procedure

1. Download the appropriate Unicode message file to your Personal Computer. For an existing translation, download the required language from https://support.avaya.com/unicode.
2. If necessary, create a new translation, or modify an existing translation, using the Avaya Message Editing Tool (AMET), available at https://support.avaya.com/amet.

   Note:

   Only the Avaya Message Editing Tool (AMET) can be used for translation edits, using any other editor will not update the Phone Message File correctly and such files will fail to install. See the *Avaya Message Editing Tool (AMET) Job Aid* in the Generic Phone Message Package file for more details on using AMET.
3. Transfer the Phone Message file to an Avaya Server that is running Communication Manager 2.2 or later, using the Avaya Web pages, the Avaya Installation Wizard, or ftp.
4. Install Phone Message files with the Communication Manager System Management Interface (SMI). The Avaya Installation Wizard only supports install of Unicode Phone Message files. Note that the Installation Wizard is the same wizard that you use to transfer Phone Message files to an Avaya Server that is running Communication Manager 2.2 or later.
5. The strings in a Communication Manager Phone Message File (avaya_unicode[2-4].txt, custom_unicode[2-4].txt, avaya_user-defined.txt, custom_user-defined.txt) are loaded in

real-time into Communication Manager memory after you click the Install button on the “Communication Manager Phone Message File” page of Communication Manager SMI.

6. Set the **Display Language** field on the Station screen to `unicode`. Note that the **Station** screen displays the unicode keyword only if a Unicode-capable telephone is entered in the Station screen **Type** field. To use a user-defined file, set the **Display Language** field on the Station screen to `user-defined`.

   Note:

   There is no uninstall option for Phone Message files. You can reload a new Phone Message file. This will overwrite existing Phone Message files.

Checking the Status of Phone Message File Loads

To verify that a Unicode Phone Message file is loaded correctly, run `status station xxxx` on any administered station. If the Unicode Phone Message file is loaded correctly, the **Display Messages Scripts** field on the second page contains the scripts that are in this file. The General Status screen for stations contains three Unicode script-related fields. To access the General Status screen, type `status station xxxx`, where xxxx is the extension of the station. The system displays the General Status screen. Click **Next** to display page 2 of the screen.

“Scripts” are a collection of symbols used to represent text in one or more writing systems. The three script fields shown in the UNICODE DISPLAY INFORMATION section are as follows:

- **Native Name Scripts**: Scripts supported in the Unicode station name.
- **Display Messages Scripts**: The scripts used in the Unicode Display Language.
- **Station Supported Scripts**: The scripts supported in the IP station that is registered to an extension.

Unicode Native Name support

Communication Manager supports Unicode for the “Name” associated with Vector Directory Numbers (VDNs), trunk groups, hunt groups, agent login id, vector names, station names, Invalid Number Dialed Display (Feature-Related System Parameters screen) and Restricted Number Dialed Display (Feature-Related System Parameters screen). The **Unicode Name** (also referred to as Native Name and Name 2) fields are hidden fields that are associated with the name fields you administer on the respective screens for each. These fields can only be administered using 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 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
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	04000000	2E80..2EFF	CJKV Radicals Supplement	Jpan
28	08000000			ChiS
29	10000000			ChiT
30	20000000			Korn

Table continues…

Script Number	Script Tag Bit (hex)	Start Code.. End Code	Script or Block Name	SAT Screen Name
31	40000000			Viet
27	04000000	2F00..2FDF	Kangxi Radicals	Jpan
28	08000000			ChiS
29	10000000			ChiT
30	20000000			Korn
31	40000000			Viet
27	04000000	3000..303F	CJKV Symbols and Punctuation	Jpan
28	08000000			ChiS
29	10000000			ChiT
30	20000000			Korn
31	40000000			Viet
27	04000000	3040..309F	Hiragana	Jpan
27	04000000	30A0..30FF	Katakana	Jpan
29	10000000	3100..312F	Bopomofo	ChiT
32	80000000	3130..318F	Hangul Compatibility Jamo	Hang
29	10000000	31A0..31BF	Bopomofo Extended	ChiT
27	04000000	31F0..31FF	Katakana Phonetic Extensions	Jpan
27	04000000	3200..32FF	Enclosed CJK Letters and Months	Jpan
28	08000000			ChiS
29	10000000			ChiT
30	20000000			Korn
31	40000000			Viet
27	04000000	3300..33FF	CJKV Compatibility	Jpan
28	08000000			ChiS
29	10000000			ChiT
30	20000000			Korn
31	40000000			Viet
27	04000000	3400..4DBF	CJKV Unified Ideographs Extension A	Jpan
28	08000000			ChiS
29	10000000			ChiT
30	20000000			Korn
31	40000000			Viet

Table continues…

Script Number	Script Tag Bit (hex)	Start Code.. End Code	Script or Block Name	SAT Screen Name
27	04000000			Jpan
28	08000000			ChiS
29	10000000	4E00..9FFF	CJKV Unified Ideographs	ChiT
30	20000000			Korn
31	40000000			Viet
32	80000000	AC00..D7AF	Hangul Syllables	Hang
27	04000000			Jpan
28	08000000			ChiS
29	10000000	F900..FAFF	CJK Compatibility Ideographs	ChiT
30	20000000			Korn
31	40000000			Viet
	00000100	FB50..FDFF	Arabic Presentation Forms-A	Arab
27	04000000			Jpan
28	08000000			ChiS
29	10000000	FE30..FE4F	CJK Compatibility Forms	ChiT
30	20000000			Korn
31	40000000			Viet
	00000100	FE70..FEFF	Arabic Presentation Forms-B	Arab
26	02000000	FF00..FFEF	Halfwidth and Fullwidth Forms	Kana

Administering displays for QSIG trunks

About this task

Proper transmission of QSIG name data for display requires certain settings in the Trunk Group screen, the Signaling Group screen, and the System-Parameters Country-Options screen.

Procedure

1. Make the following changes to the Trunk Group screen.
   a. Set **Group Type** to `ISDN`
   b. Set **Character Set for QSIG Names** to `iso8859-1`
   c. Set **Outgoing Display** to `y`
   d. Set **Send Calling Number** to `y`
   e. Set **Send Name** to `y`
2. On the Signaling Group screen, set **Supplementary Service Protocol** to `b`.
3. On the System-Parameters Country-Options screen, set **Display Character Set** to `Roman`.

Fixing Problems

Symptom	Cause and Solution
Characters that display are not what you thought you entered.	This feature is case sensitive. Check the table to make sure that you entered the right case.
If you enter ~c, the system will display * instead.	Lower-case “c” has a specific meaning in Avaya Communication Manager, and therefore cannot be mapped to any other character. The system displays an asterisk “*” in its place.
If you enter ~-> or ~<-, the system does not display anything.	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.
If you enter a character with a descender then the system displays it with part of it cut off.	Some of the unused characters in Group2a have descenders that do not appear entirely within the display area. These characters are not included in the character map. For these characters (g,j,p,q,y), use Group1 equivalents.

Related Topics

See the Telephone Displays and the Administrable Display Languages feature descriptions in the *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205 for more information.

To view the dial pad letter/number/symbol mapping tables used for the integrated directory, see Telephone Display in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Setting the Directory Buttons

About this task

Your Communication Manager integrated directory contains the names and extensions that are assigned on each Station screen. Display-telephone users can use a telephone button to access the directory, use the touch-tone buttons to key in a name, and retrieve an extension from the directory.

Note:

When you assign a name beginning with two tildes (~~) to a telephone, and **Display Character Set** on the System Parameters Country-Options screen is set to Roman, the name does not appear in the integrated directory. Note that this is the only way to hide a name in the integrated directory.

The example below shows how to assign directory telephone buttons for extension 2000.

Our button assignment plan is set up so that telephone buttons 6, 7, and 8 are used for the directory. Remember, the name you type in the **Name** field on the first page of the Station screen is the name that the system will display when the integrated directory is accessed on a telephone display, except when the name is “hidden”, as described in the Note above.

Procedure

1. Type `change station 2000`.
2. Press `Enter`.
3. Press `Next Page` to move to the BUTTON ASSIGNMENTS section on Station screen (page 4).
4. In **Button Assignment** field 6, type `directory`.
5. In **Button Assignment** field 7, type `next`.
6. In **Button Assignment** field 8, type `call-display`.
7. Press `Enter` to save your changes.

Chapter 10: Handling Incoming Calls

Basic Call Coverage

Basic incoming call coverage:

- Provides for automatic redirection of calls to alternate destinations when the called party is unavailable or not accepting calls
- Provides the order in which Communication Manager redirect calls to alternate telephones or terminals
- Establishes up to 6 alternate termination points for an incoming call
- Establishes redirection criteria that govern when a call redirects
- Redirects calls to a local telephone number (extension) or an off-switch telephone number (public network)

Redirection

Call coverage allows an incoming call to redirect from its original destination to an extension, hunt group, attendant group, uniform call distribution (UCD) group, direct department calling (DDC) group, automatic call distribution (ACD) split, coverage answer group, Audio Information Exchange (AUDIX), or vector for a station not accepting calls.

You can force a call to follow a coverage path more quickly using the Send All Calls feature. Send All Calls can be enabled using a button or a feature access code.

The **Send All Calls** button has an **Ext** sub-field. The **Ext** sub-field allows you to apply Send All Calls to a station other than the station on which the button is configured. For example, you can have a Send All Calls button that applies to station X, and you can use it to activate Send All Calls on behalf of X.

Administering system-wide call coverage characteristics

About this task

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

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

Procedure

1. Leave all default settings as they are set for your system.
2. If you require to customize your system, carefully read and understand each field description before you make any changes.

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

For information on setting the Caller Response Interval before a call goes to coverage, see “Caller Response Interval” in the Call Coverage section of *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Creating coverage paths

About this task

This section explains how to administer various types of call coverage. In general, call coverage refers to what happens to incoming calls. You can administer paths to cover all incoming calls, or define paths for certain types of calls, such as calls to busy telephones. You can define where incoming calls go if they are unanswered 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 unanswered, and finally access a voice mailbox if the receptionist is unavailable.

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 unavailable, the call proceeds to the next coverage point regardless of the type of coverage administered in the point that was unavailable. For example, if the unavailable coverage point has a hunt group coverage path administered, the hunt group coverage path would not be used by a call coming into the hunt group through the higher-level coverage path. The hunt group coverage path would be used only for calls coming directly into the hunt group extension.

Procedure

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

   The system displays the Coverage Path screen. The system displays the next undefined coverage path in the sequence of coverage paths. Our example shows coverage path number 2.

3. Type a coverage path number in the **Next Path Number** field.

   The next path is optional. It is the coverage path to which calls are redirected if the current path’s coverage criteria does not match the call status. If the next path’s criteria matches the call status, it is used to redirect the call; no other path is searched.

4. Fill in the **Coverage Criteria** fields.

You can see that the default sets identical criteria for inside and outside calls. The system sets coverage to take place from a busy telephone, if there is no answer after a certain number of rings, or if the **DND** (do not disturb), **SAC** (send all calls), or **Go to Cover** button has been pressed or corresponding feature-access codes dialed.

5. Fill in the **Point** fields with the extensions, hunt group number, or coverage answer group number you want for coverage points.

   Each coverage point can be an extension, hunt group, coverage answer group, remote number, or attendant.

6. Click **Enter** to save your changes.

Tip:

If you want to see which extensions or groups use a specific coverage path, type `display coverage sender group n`, where `n` is the coverage path number. For example, you should determine which extensions use a coverage path before you make any changes to it.

Assigning a coverage path to users

About this task

Once you create a coverage path, assign it to a user. For example, we will assign the new coverage path to extension 2045.

Note:

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

Procedure

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

   The system displays the Station screen for extension 2054.

3. Type `2` in the **Coverage Path 1** field.

   To give extension 2054 another coverage path, you can type a coverage path number in the **Coverage Path 2** field.

4. Press `Enter` to save your changes.

Advanced call coverage

Advanced incoming call coverage:

- redirects calls based on time-of-day.
- allows coverage of calls that are redirected to sites not on the local server running Communication Manager.

- allows users to change back and forth between two coverage choices (either specific lead coverage paths or time-of-day tables).

Covering calls redirected to an off-site location

Before you begin

- On the System Parameters Customer-Options (Optional Features) screen, verify the **Coverage of Calls Redirected Off-Net Enabled** field is y. If not, go to the Avaya Support website at http://support.avaya.com.
- You need call classifier ports for all situations except ISDN end-to-end signaling, in which case the ISDN protocol does the call classification. For all other cases, use one of the following:
  - Tone Clock with Call Classifier - Tone Detector circuit pack. See the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207 for more information on the circuit pack.
  - Call Classifier - Detector circuit pack.

About this task

You can provide coverage for calls that have been redirected to an off-site location (for example, your home). You can use the capability, called Coverage of Calls Redirected Off-Net (CCRON) to redirect calls onto the public network and bring back unanswered calls for further coverage processing.

Procedure

1. Type `change system-parameters coverage-forwarding`.
2. Press `Enter`.
3. Click **Next Page** until you see the **Coverage of Calls Redirected Off-Net (CCRON)** page of the System-Parameters Coverage-Forwarding screen.
4. In the **Coverage of Calls Redirected Off-Net Enabled** field, type `y`.

   This instructs Avaya Communication Manager to monitor the progress of an off-net coverage or off-net forwarded call and provide further coverage treatment for unanswered calls.
5. In the **Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point** field, leave the default as y.
6. In the **Ignore Network Answer Supervision** field, leave the default as n.
7. Click **Enter** to save your changes.

Defining coverage for calls redirected to external numbers

About this task

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

You can use Standard remote coverage to an external number to send a call to an external telephone, but does not monitor the call once it leaves your system. Therefore, if the call is busy or unanswered at the external number, the call cannot be pulled back to the system. With standard remote call coverage, make the external number the last coverage point in a path.

Note:

Using remote coverage, you cannot cover calls to a remote voice mail.

With newer systems, you might have the option to use the Coverage of Calls Redirected Off-Net feature. If this feature is active and you use an external number in a coverage path, the system can monitor the call to determine whether the external number is busy or does not answer. If necessary, the system can redirect a call to coverage points that follow the external number. With this feature, you can have a call follow a coverage path that starts at the user's extension, redirects to the user's home telephone, and if unanswered 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, define the number in the Remote Call Coverage Table and then use the remote code in the coverage path.

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

Procedure

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

   The system displays the Remote Call Coverage Table screen.
3. In one of the remote fields, type the number that you want to assign to the remote coverage point. You can enter up to 16 digits, or leave the field blank. In this example, the number used is 93035381000.

   If you want to place a call outside of your network, add the digit that is used as Auto Alternate Routing (AAR) Access Code before the external number. In this example, dial 9 to place outside calls.
4. Note down the remote code number that you use for the external number.
5. Save the changes.
6. Type `change coverage path` *`n`*, where `n` is the coverage path number.
7. Press `Enter`.

   The system displays the Coverage Path screen.

   Tip:

   Before making changes, you can use `display coverage sender group` *`n`*, to determine which extensions or groups use path *n*.
8. In the **Coverage Point** field, type the remote code number that you use for the external number.

9. Save the changes.

   Note:

   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.

   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 unanswered 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).

   For more information on coverage, see Call Coverage in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Defining time-of-day coverage

About this task

The Time of Day Coverage Table on your system lets you redirect calls to coverage paths according to the time of day and day of the week when the call arrives. You need to define the coverage paths you want to use before you define the time of day coverage plan.

For example, let us say you want to administer the system so that incoming calls to extension 2054 redirect to a coworker in the office from 8:00 a.m. to 5:30 p.m., and to a home office from 5:30 p.m. to 8:00 p.m. on weekdays. You want to redirect the calls to voice mail after 8:00 p.m. weekdays and on weekends.

Procedure

1. Type `add coverage time-of-day next`.
2. Press `Enter`.

   The system displays the Time of Day Coverage Table screen, and selects the next undefined table number in the sequence of time-of-day table numbers. If this is the first time-of-day coverage plan in your system, the table number is 1.

   Record the table number so that you can assign it to extensions later.

3. To define your coverage plan, enter the time of day and path number for each day of the week and period of time.

   Enter time in a 24-hour format from the earliest to the latest. For this example, assume that coverage path 1 goes to a coworker, path 2 to home, and path 3 to voice mail.

   Define your path for the full 24 hours (from 00:01 to 23:59) in a day. If you do not list a coverage path for a period of time, the system does not provide coverage for that time.

4. Click **Enter** to save your changes.
5. Now assign time-of-day coverage to a user. For example, we use extension 2054:
   a. Type `change station nnnn`, where `nnnn` is the extension number.

b. Press `Enter`.

   The system displays the Station screen.

c. Move your cursor to Coverage Path 1 and type t plus the number of the Time of Day Coverage Table.

d. Click **Enter** to save your changes.

Now calls to extension 2054 redirect to coverage depending on the day and time that each call arrives.

Creating coverage answer groups

About this task

You can create a coverage answer group so that up to 100 telephones simultaneously ring when calls cover to the group. Anyone in the answer group can answer the incoming call.

Procedure

1. Enter `add coverage answer-group next`.
2. In the **Group Name** field, enter a name to identify the coverage group.
3. In the **Ext** field, type the extension of each group member.
4. Save the new group list.

   The system automatically completes the **Name** field when you save the changes.

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. Call Forwarding can be enabled using a button or a feature access code.

All **Call Forward** buttons have an **Ext** sub-field. The **Ext** sub-field allows you to apply Call Forward button to a station other than the station on which the Call Forward button is configured. For example, you can have a Call Forward button that applies to station X, and you can forward calls on behalf of X.

Within each class of service, you can determine whether the users in that COS have the following call forwarding features:

- Call Forwarding All Calls — Users can use this to redirect all incoming calls to an extension, attendant, or external telephone number.

- Call Forwarding Busy/Don’t Answer — Users can use this to redirect calls only if their extensions are busy or they do not answer.
- Restrict Call Fwd-Off Net — This 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 unanswered, redirect to the forwarding number, set this parameter to 4.

You also can use the System Parameters Call Coverage/Call Forwarding screen to determine whether the forwarded-to telephone can override call forwarding to allow calls to the forwarded-from telephone (Call Forward Override). For example, if an executive forwards incoming calls to an attendant and the attendant needs to call the executive, the call can be made only if the **Call Forwarding Override** field is set to y.

Determining extensions having call forwarding activated

Procedure

1. Type `list call-forwarding`.
2. Press `Enter`.

   This command lists all the extensions that are forwarded along with each forwarding number.

   Note:

   If you have a V1, V2, or V3 system, you can see if a specific extension is forwarded only by typing `status station nnnn`, where `nnnn` is the specific extension.

   For more information see “Call Forwarding” in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Setting up call forwarding for users

About this task

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

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

Procedure

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

   The system displays the Feature Access Code (FAC) screen.
3. In the **Call Forwarding Activation Busy/DA** field, type `*70`.

The *70 feature access code activates the call forwarding option so incoming calls forward when your telephone is busy or does not answer.

4. In the **Call Forwarding Activation All** field, type `*71`.

   The *71 feature access code forwards all calls.

5. In the **Call Forwarding Deactivation** field, type `#72`.

   The #72 feature access code deactivates the call forwarding option.

6. Press `Enter` to save your changes.
7. Type `change cos`.
8. Press `Enter`.

   The system displays the Class of Service screen.

9. On the **Call Fwd-All Calls** line, in the 1 column, type `y`.

   With this the user with this Class of Service can forward their calls. The 1 column is for telephones with a Class of Service of 1.

10. On the **Console Permissions** line, in the 1 column, type `y`.

    With this the user can define call forwarding on any station, not just the dialing station.

11. On the **Restrict Call Fwd-Off Net** line, in the 1 column, type `y`.

    This restricts your users from forwarding calls off-site. If you want your users to be able to call off-site, leave this field as n.

12. On the **Call Forward Busy/DA** line, in the 1 column, type `y`.

    This forwards a user's calls when the telephone is busy or doesn't answer after a programmed number of rings.

13. Press `Enter` to save your changes.

Allowing users to specify a forwarding destination

About this task

Now that you have set up system-wide call forwarding, have your users use this procedure if they want to change their call forwarding destination from their work (local) station.

Procedure

1. They dial either their Call Forwarding Activation Busy/DA or Call Forwarding Activation All feature access code. If your users have buttons assigned, they press those buttons, listen for dial tone, and dial the digits.

   Note:

   Both Call Forwarding Activation Busy/DA or the Call Forwarding Activation All cannot be active for the same telephone at the same time.

In this example, enter `*71` for Call Forwarding Activation All.

2. They dial their "forwarding-to" off-site or on-site number.

   In this example, enter `2081`. This is a local number; for off-site forwarding, include the AAR/ ARS feature access code.

3. When they hear the 3-beep confirmation tone, they disconnect.

Changing the forwarding destination remotely

About this task

Now that you have set up all of the required system administration for call forwarding, have your users use this procedure if they want to change their call forwarding destination from a telecommuting (off-site) telephone.

Procedure

1. They dial their telecommuting extension.

   In this example, enter `555-9126`.

2. When they get dial tone, they dial either their Extended Call Forward Activate Busy/DA or the Extended Call Forward Activate All feature access code.

   In this example, enter `*61` for the Extended Call Forward Activate All number.

3. When they get dial tone, they dial their extension number. Press the `#`.

   In this example, enter `1014`, then `#`.

4. Even though there is no dial tone, they dial their security code. Press `#`.

   In this example, enter `4196`, then `#`.

5. When they get dial tone, they dial their "forwarding-to" off-site or on-site number.

   In this example, enter `9-555-2081`.

6. When they hear the 3-beep confirmation tone, they disconnect.

Allowing users to change coverage remotely

About this task

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

Procedure

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

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

3. In the **Change Coverage Access Code** field, type `*85`.

   Use the *85 feature access code to change a coverage path from a telephone or remote station.

4. Press `Enter` to save your changes.
5. Type `change cor`.
6. Press `Enter`.

   The system displays the Class of Restriction screen.

7. In the **Can Change Coverage** field, type `y`.

   This permits users to select one of two previously administered coverage paths.

8. Press `Enter` to save your changes.
9. Type `change station 1014`.
10. Press `Enter`.

    The system displays the Station screen for extension 1014.

11. In the **Security Code** field, type `4196`.

    In this example, this is your security code.

12. In the **Coverage Path 1** and **Coverage Path 2** fields, verify that both are defined enabling your user to move from one coverage path to another.

    The t1 and t2 are the numbers of the Time of Day Coverage Tables.

13. Press `Enter` to save your changes.

Enhanced Call Forwarding

There are three types of Enhanced Call Forwarding:

- Use Enhanced Call Forwarding Unconditional to forward all calls
- Use Enhanced Call Forwarding Busy to forward calls when the user’s line is busy
- Use Enhanced Call Forwarding No Reply to forward calls when the user does not answer the call

The user can activate or deactivate any of these three types from their 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.

Redirection

Call coverage allows an incoming call to redirect from its original destination to an extension, hunt group, attendant group, uniform call distribution (UCD) group, direct department calling (DDC) group, automatic call distribution (ACD) split, coverage answer group, Audio Information Exchange (AUDIX), or vector for a station not accepting calls.

Activating Enhanced Call Forwarding Using a feature button

Procedure

1. Press the feature button labeled cfwd-enh

   The 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.

Activating Enhanced Call Forwarding Using a feature access code

Procedure

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 using a feature button

Procedure

1. On the telephone, press the feature button labeled **cfwd-enh**.

   The telephone goes off hook.

2. Press 2 to deactivate Enhanced Call Forwarding.

3. On the telephone keypad, press the following numbers for different call forwarding scenarios:
   - 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. On the telephone keypad, press the following numbers for the type of calls to be forwarded:
   - 1 for internal calls.
   - 2 for external calls.
   - 3 for all calls.

   You hear a confirmation tone.

Deactivating enhanced call forwarding using a feature access code

Procedure

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 using a feature button

Procedure

1. On the telephone, press the feature button labeled **cfwd-enh**.

   The telephone goes off hook.
2. Press 1 to reactivate the Enhanced Call Forwarding feature.
3. Press one of the following numbers for the required call forwarding option.
   - 1 for Enhanced Call Forwarding Unconditional.
   - 2 for Enhanced Call Forwarding Busy.
   - 3 for Enhanced Call Forwarding No Reply.

4. Press one of the following numbers for the required call type.
   - 1 to forward internal calls.
   - 2 to forward external calls.
   - 3 to forward all calls.
5. Optionally, dial the destination number to which calls must be forwarded.

   If you do not enter a destination number, the previous destination number will be used.

   At the end of an external destination number, dial # at the end of an external destination number, or wait for the timer to expire.

   You hear a confirmation tone.

Reactivating enhanced call forwarding using a feature access code

Procedure

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 using a feature button

Procedure

1. On the telephone, press the feature button labeled **cfwd-enh**.

   The telephone goes off hook.
2. Press 3 to display the enhanced call forwarding status.

   Your telephone displays the status of the Enhanced Call Forwarding options.

Displaying Enhanced Call Forwarding Status Using a Feature Access Code

Procedure

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 enhanced call forwarding from an off-the-network telephone

Before you begin

Set the **Console Permissions** field on the Class of Service screen to `y`.

Procedure

1. Dial the remote access number, including barrier code or authentication code.
2. Dial the feature access code to activate the Enhanced Call Forwarding feature.
3. Press one of the following numbers for the required enhanced call forwarding options:
   - `1` for Enhanced Call Forwarding Unconditional.
   - `2` for Enhanced Call Forwarding Busy.
   - `3` for Enhanced Call Forwarding No Reply.
4. Press one of the following numbers for the required call type:
   - `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.

   Note:

   After dialing the external destination number, press the pound key (`#`) or wait for the timer to expire.

   The system generates the confirmation tone.

Deactivating enhanced call forwarding from an off-the-network telephone

Before you begin

Set the **Console Permissions** field on the Class of Service screen to `y`.

Procedure

1. Dial the remote access number, including barrier code or authentication code.
2. Press the feature access code for deactivating the enhanced call forwarding feature.
3. Press one of the following numbers for the required call forwarding options:
   - `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 one of the following numbers for the required call type:
   - `1` for internal calls.
   - `2` for external calls.
   - `3` for all calls.
5. Dial the forwarding station extension.
6. Dial the destination number to which calls must be forwarded.

   Note:

   After dialing the external destination number, dial the pound key (`#`) or wait for the timer to expire.

   The system generates the confirmation tone.

Activating enhanced call forwarding from a telephone with console permissions

Procedure

1. On the telephone, press the feature access code for activating the Enhanced Call Forwarding feature.

   The telephone goes off-hook.
2. Press one of the following numbers for the required call type:
   - `1` to forward internal calls.
   - `2` to forward external calls.

- 3 to forward all calls.

3. Dial the forwarding station extension.
4. Dial the destination number to which calls will be forwarded.

Note:

At the end of an external destination number, dial hash (#) or wait for the timer to expire.

You hear a confirmation tone.

Deactivating enhanced call forwarding from a telephone with console permissions

Procedure

1. On the telephone, press the feature access code for deactivating the enhanced call forwarding feature.

   The telephone goes off hook.
2. Press one of the following numbers for the required enhanced call forwarding options:
   - 0 for all Enhanced Call Forwarding.
   - 1 for Enhanced Call Forwarding Unconditional.
   - 2 for Enhanced Call Forwarding Busy.

   You hear a confirmation tone.

Night Service

You can use night service to direct calls to an alternate location when the primary answering group is unavailable. For example, you can administer night service so that anyone in your marketing department can answer incoming calls when the attendant is at lunch or has left for the day.

Once you administer night service to route calls, your end-users merely press a button on the console or a feature button on their telephones to toggle between normal coverage and night service.

There are five types of night service:

- Night Console Night Service — directs all attendant calls to a night or day/night console
- Night Station Night Service — directs all incoming trunk or attendant calls to a night service destination
- Trunk Answer from Any Station (TAAS) — directs incoming attendant calls and signals a bell or buzzer to alert other employees that they can answer the calls

- Trunk Group Night Service — directs incoming calls to individual trunk groups to a night service destination
- Hunt Group Night Service — directs hunt group calls to a night service destination

Setting up night station service to voice mail

About this task

The night station service (also known as Listed Directory Number (LDN) Night Service) sends calls directed to an LDN to voice mail when the system is in night service.

What is described below is a common setup; however, you can use a regular extension in this field, but it will not follow coverage.

Note:

You can use a dummy hunt group (one with no members) or an exported station with a coverage path. The instructions below use a hunt group.

Procedure

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

   The system displays the Hunt Group screen.

   The **Group Number** field fills automatically with the next hunt group number.
3. In the **Group Name** field, type the name of the group.

   In our example, type `ldn nights`. There should be no members in this hunt group.
4. Click **Enter** to save your changes.

   Note:

   If you are using tenant partitioning, the command for the next step will be `change tenant x`. If you are using tenant partitioning, the **Night Destination** field does not appear on the Listed Directory Numbers screen. Instead, it is on the Tenant screen.
5. Type `change listed-directory-numbers`.
6. Press `Enter`.

   The system displays the Listed Directory Numbers screen.
7. In the **Night Destination** field, add the night destination on the listed directory telephone.

   In our example, type `51002`.
8. Click **Enter** to save your changes.
9. Type `change console-parameters`.
10. Press `Enter`.

    The system displays the Console Parameters screen.

11. In the **DID-LDN Only to LDN Night Ext** field, type `n`.
12. Click **Enter** to save your changes.
13. From a telephone with console permissions, dial the call forwarding feature access code, then the hunt group's extension, followed by the main number of AUDIX.

    In our example, dial 51002.

    Note:

    You should receive the confirmation tone (3 beeps). This step is very important as calls to the LDN night service extension do not follow coverage.
14. In voice mail, build your auto attendant with the extension of the Listed Directory Number, not the hunt group.

    The originally dialed number was the LDN. That is what Communication Manager passes to the voice mail. In the case of the INTUITY and newer embedded AUDIX Voice Mail systems, you can use the Auto Attendant routing table to send the calls to a common Auto Attendant mailbox.

Setting up night console service

About this task

Night Console Service directs all calls for primary and daytime attendant consoles to a night console. When you activate 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.

To activate and deactivate Night Console Service, press the Night Service button on the principal attendant console or designated console.

Only the principal console can activate night service. In the absence of any console, a telephone can activate night service.

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

Procedure

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

   The system displays the Attendant Console screen.
3. In the **Console Type** field, type `principal`.

   There can be only one night-only or one day/night console in the system unless you administer Tenant Partitioning. Night Service is activated from the principal console or from the one station set per-system that has a **nite-serv** button.

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

Setting up night station service

About this task

You can use night station service if you want to direct incoming trunks calls, DID-LDN (direct inward dialing-listed directory number) calls, or internal calls to the attendant (dialed ‘O’ calls) to a night service destination.

Let us say your attendant, who answers extension (LDN) 8100, usually goes home at 6:00 p.m. When customers call extension 8100 after hours, you would like them to hear an announcement that asks them to try their call again in the morning.

To set up night station service, you need to record the announcement (in our example, it is recorded at announcement extension 1234).

Tip:

All trunk groups that are routed through the attendant direct to this night service destination provided they already do not have a night service destination and, on the Console Parameters screen, the **DID-LDN Only to DID-LDN Night Ext** field is n. See *Setting up trunk answer from any station*.

Procedure

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

   The system displays the Listed Directory Numbers screen.
3. Enter `1234` in the **Night Destination** field.

   The destination can be an extension, a recorded announcement extension, a vector directory number, or a hunt group extension.
4. Click **Enter** to save your changes.
5. Type change console-parameters.
6. Press Enter.

   The system displays the Console Parameters screen.
7. In the **DID-LDN Only to LDN Night Extension** field, type `n`.
8. Click Enter to save your changes.

   After you set up night station service, have the attendant use the night console button to activate and deactivate night service.

Setting up trunk answer from any station

About this task

There might be situations where you want everyone to be able to answer calls when the attendant is away. Use trunk answer any station (TAAS) to configure the system so that it notifies everyone

when calls are ringing. Then, you can give users the trunk answer any station feature access code so they can answer these calls.

When the system is in night service mode, attendant calls redirect to an alerting device such as a bell or a buzzer. This lets other people in the office know when they should answer the telephone.

Note:

If no one answers the call, the call will not redirect to night service.

We will define a feature access code (we'll use 71) and configure the alerting device for trunk answer any station.

You need a ringing device and 1 port on an analog line circuit pack. See the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207, for more information on the circuit pack.

Procedure

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

   The system displays the Feature Access Code (FAC) screen.
3. Click **Next** until you see the T**runk Answer Any Station Access Code** field.
4. In the **Trunk Answer Any Station Access Code** field, type `71`.
5. Click **Enter** to save your changes.

   Once you set the feature access code, determine where the external alerting device is connected to the Communication Manager server (we'll use port 01A0702).

   To set up external alerting:
6. Type `change console-parameters`.
7. Press `Enter`.

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

   Use the port address assigned to the external alerting device.
9. In the **EXT Alert Port (TAAS)** field, type `01A0702`.
10. Click **Enter** to save your changes.

Setting up external alerting

Procedure

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

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

Use the port address assigned to the external alerting device.

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

Setting up external alerting night service

About this task

Calls redirected to the attendant via Call Forwarding or Call Coverage will not go to the LDN Night Station. If there is no night station specified, and the TAAS bell is being used, these calls ring the TAAS bell. A call following the coverage path rings the TAAS bell for the number of times indicated in the Coverage Don't Answer Interval for Subsequent Redirection (Rings) field. If unanswered, the call proceeds to the next point in the station's coverage path. If the call was sent to the Attendant by Call Forwarding, it continues to ring the TAAS bell.

When night service is enabled, and there is a night service destination on the Listed Directory Numbers screen, calls covering to the attendant attempt to ring the night destination instead of the attendant position even if the handset is plugged in.

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

Procedure

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

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

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

   This is the port address assigned to the external alerting device.
8. Click **Enter** to save your changes.

   The system is in Night Service.

   Any calls to extension 2000 now go to extension 3000 (the guard's desk).

   Any "0" seeking calls go to extension 3000 (the guard's desk).

Sending LDN calls to the attendant during the day and to the TAAS bell at night

Procedure

1. Type `change console-parameters`.

2. Press `Enter`.

   The system displays the Console Parameters screen.

3. In the **DID-LDN Only to Night Ext?**field, type `y`.

   Using this only listed directory number calls (LDN) go to the listed directory night service number extension.

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

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

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

   Any DNIS extension 2000 calls now go to the TAAS bell.

   Any “0” seeking calls now go to the TAAS bell.

Setting up trunk group night service

About this task

You can use trunk group night service if you want to direct individual trunk groups to night service. The system redirects calls from the trunk group to the group’s night service destination.

Trunk group night service overrides night station service. For example, we will say you activate trunk group night service, and then your attendant activates night station service. In this case, calls to the trunk group use the trunk night service destination, rather than the station night service destination.

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

Procedure

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

   The system displays the Trunk Group screen.

3. Type `1245` in the **Night Service** field.

   The destination can be a station extension, a recorded announcement extension, a vector directory number, a hunt group extension, a terminating extension group, or attd if you want to direct the call to the attendant.

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

Setting up night service for hunt groups

About this task

You can administer hunt group night service if you want to direct hunt group calls to a night service destination.

Let us say your helpline on hunt group 3 does not answer calls after 6:00 p.m. When customers call after hours, you would like them to hear an announcement that asks them to try their call again in the morning.

To set up night service for your helpline, you need to record the announcement (in our example, the announcement is on extension 1234) and then modify the hunt group to send calls to this extension.

Procedure

1. Type `change hunt-group`.
2. Press `Enter`.

   The system displays the Hunt Group screen for hunt group 3.
3. In the **Night Service Destination** field, type `1234`.

   The destination can be an extension, a recorded announcement extension, a vector directory number, a hunt group extension, or attd if you want to direct calls to the attendant.

   Calls to hunt group 3 will follow the coverage path assigned to extension 1234.
4. Click **Enter** to save your changes.
5. Now you need to program a night service button.

Related links

Hunt Groups on page 246

Deactivating the Night Service feature

Before you begin

Ensure that you have the console permissions, that is, the **Console permission** field on COS is set to `y` for the designated station.

Procedure

To deactivate the Night Service feature, disable the Night Service feature button on the principal attendant console or on the designated phone.

Call Pickup

Users might need to answer a call that is ringing at a nearby desk. With Communication Manager, a user can answer a call that is ringing at another telephone in three ways:

- Use Call Pickup. With Call Pickup, you create one or more pickup groups. A pickup group is a collection, or list, of individual telephone extensions. A pickup group is the way to connect individual extensions together. For example, if you want everyone in the payroll department to be able to answer calls to any other payroll extension, you can create a pickup group that contains all of the payroll extensions.

A user extension can belong to only one pickup group. Also, the maximum number of pickup groups might be limited by your system configuration.

Using their own telephones, all members in a pickup group can answer a call that is ringing at another group member telephone. If more than one telephone is ringing, the system selects the extension that has been ringing the longest.

- Use Extended Call Pickup. With Extended Call Pickup, you can define one or more extended pickup groups. An extended pickup group is the way to connect individual pickup groups together.

  There are two types of extended pickup groups: simple and flexible. You administer the type of extended pickup groups on a system-wide basis. You cannot have both simple and flexible extended pickup groups on your system at the same time.

  Based on the type of extended pickup group that you administer, members in one pickup group can answer calls to another pickup group.

  For more information, see *Setting up simple extended pickup groups*, *Setting up flexible extended pickup groups*, and *Changing extended pickup groups*.
- Use Directed Call Pickup. With Directed Call Pickup, users specify what ringing telephone they want to answer. A pickup group is not required with Directed Call Pickup. You must first administer Directed Call Pickup before anyone can use this feature.

For more information, see *Setting up Directed Call Pickup*.

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

Call Pickup Alert

Members of a call pickup group know that another group member is receiving a call in two ways:

- Group members can hear the other telephone ring.
- The Call Pickup button status lamp on the telephones of all the group members flash.

Note:

You must activate Call Pickup Alerting in your system, and assign a Call Pickup button to the telephones of each pickup group member, before the Call Pickup button status lamps work properly.

For information on how to set up Call Pickup Alerting, see Enabling Call Pickup Alerting.

If the **Call Pickup Alerting** field on the Feature-Related System Parameters screen is set to n, members of the call pickup group must rely only on ringing to know when another group member receives a call. Pickup group members must be located close enough that they can hear the ringing of the other telephones.

To answer a call, a pickup group member can either press the Call Pickup button on the telephone, or dial the Call Pickup feature access code (FAC).

For more information, see Assigning a Call Pickup button to a user telephone, and Assigning a Call Pickup feature access code.

The Call Pickup Alerting feature is enhanced to support the SIP telephones. You need to upgrade the SIP telephone firmware 2.6 to take advantage of call pickup alerting on SIP telephones. You can activate an audible and a visual alert at a SIP telephone by administering the **Call Pickup Ring Type** and **Call Pickup Indication** fields available under the Screen and Sound Options menu on the SIP telephones.

For more information on how to administer the audible and visual alerting, see the user guide for your SIP telephone.

The **Call Pickup Alerting** field on the Feature-Related System Parameters screen determines how the Call Pickup button status lamps operate.

- If the **Call Pickup Alerting** field is set to n, the Call Pickup Button status lamps on all pickup group member telephones do not flash when a call comes in. When a pickup group member hears the telephone of another group member ring and presses the Call Pickup button to answer the call, the:
  - Call Pickup button status lamp of the answering group member becomes steadily lit for the duration of the call.
  - Telephone of the called group member stops ringing.
- If the **Call Pickup Alerting** field is set to y, the Call Pickup Button status lamps on all pickup group member telephones flash when a call comes in. When a pickup group member sees the Call Pickup button status lamp flash and presses the Call Pickup button to answer the call, the:
  - Call Pickup button status lamp of the answering group member goes out.
  - Call Pickup button status lamp of the called group member goes out.
  - Call Pickup button status lamps of the other pickup group members go out.
  - Telephone of the called group member stops ringing.

If another call comes into the pickup group,

- The call will alert to the answering group member. However, the answering group member cannot answer the call using the call pickup button unless the member puts the original call on hold. Once the group member is off the original call, that member is alerted for subsequent group calls and can answer the call using the call pickup button.
- The call alerts to all other group members and can be answered by any of these other group members.

In all scenarios, the call appearance button on the telephone of the called group member:

- Stays steadily lit if the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to y. The called group member can join the call in progress by pressing the lit call appearance button. The person who picked up the call can either stay on the call or disconnect the call.
- Goes out if the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to n. The called group member cannot join the call in progress.

The system uses an algorithm to select what call is answered when multiple calls ring or alert in a call pickup group at the same time. The system searches the extensions of the call pickup group

until the system finds an extension with a call that is eligible to be answered with Call Pickup. The system selects this call to be answered. The next time that a group member answers a call with Call Pickup, the system bypasses the extension that was answered most recently, and starts the search at the next extension.

For example, if a group member attempts to use Call Pickup when two calls are ringing at extension A and one call is ringing at extension B, the system selects the calls in the following order:

- One of the calls to extension A
- The call to extension B
- The remaining call to extension A

The system also determines which call that a group member answers when multiple calls ring or alert at the same telephone. The system selects the call with the lowest call appearance, which is usually the call appearance that is nearest to the top of the telephone.

For example, when calls ring or alert at the second and the third call appearances, the system selects the call on the second call appearance for the user to answer.

With Communication Manager Release 6.3.6, call pickup alerting has changed. If the calling station and the called station belong to the same pickup group, both the stations will not get the pickup notification. However, other members of the pickup group will receive the notification. This behavior is applicable to all types of stations, such as DCP, H.323, and SIP. For example, Station A, Station B, and Station C are in a pickup group. If Station A is used to call to Station B, Station C will get the pickup notification. But, Station A and Station B will not get the pickup notification.

Setting up Call Pickup

About this task

The first step in setting up any call pickup system is to create pickup groups and assign users to the groups. You can create one or many pickup groups, depending on your needs. A user extension can belong to only one pickup group.

In this exercise, you will:

- Add a pickup group and assign users to the pickup group.
- Enable Call Pickup alerting.
- Assign a Call Pickup button to each extension in the pickup group.
- Assign a feature access code (FAC).

Adding Pickup Groups

Procedure

1. Type `add pickup-group next`.
2. Press `Enter`.

   The system displays the Pickup Group screen. The system also assigns the next available Group Number for the new pickup group.

Note:

The **Extended Group Number** field is not shown in this example because the system is set for none or simple extended pickup groups. For more information, see *Setting up simple extended pickup groups*. If the **Extended Group Number** field is visible on this screen, then your system is set up for flexible extended pickup groups.

For more information, see *Setting up flexible extended pickup groups*.

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

   Up to 50 extensions can belong to one pickup group.
5. Click **Enter** to save your changes.

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

Example

This procedure shows how to set up a new pickup group 11 for Accounting. For the rest of these procedures, let us say that you also set up these pickup groups:

- 12 for Billing
- 13 for Credit Services
- 14 for Delinquency Payments
- 15 for Executives
- 16 for Finance

Related links

Simple extended pickup groups on page 237
Flexible Extended Pickup Groups on page 239

Enabling Call Pickup Alerting

About this task

With Call Pickup Alerting, members of pickup groups know visually when the telephone of another member is ringing. Use Call Pickup Alerting if the telephones of other pickup group members are too far away to be heard. You must enable Call Pickup Alerting in your system.

Procedure

1. Enter `change system-parameters features`.
2. Click **Next** until you see the **Call Pickup Alerting** field.
3. Set the **Call Pickup Alerting** field to `y`.
4. Select **Enter** to save your changes.

Related links

Call Pickup Alert on page 229

Assigning a Call Pickup button to a user telephone

About this task

After you define one or more pickup groups, assign a Call Pickup button for each extension in each pickup group. Users in a pickup group can press the assigned Call Pickup button to answer calls to any other extension in their pickup group.

Procedure

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

   The system displays the Station screen.
3. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
4. Type `call-pkup` after the button number.
5. Press **Enter** to save your changes.

   Repeat this procedure for each member of each pickup group.

Assigning a Call Pickup feature access code

About this task

After you define one or more pickup groups, assign and give each member the Call Pickup feature access code (FAC). Instead of using the Call Pickup button, users in a pickup group can dial the assigned FAC to answer calls to any other extension in their pickup group.

Procedure

1. Enter `change feature-access-codes`.
2. In the **Call Pickup Access Code** field, type the required FAC.

   Make sure that the FAC complies with your dial plan.
3. Select **Enter** to save your changes.

Removing a user from a call pickup group

Procedure

1. Enter `change pickup-group n`, where *n* is the number of the pickup group.
2. Move to the extension that you want to remove.
3. Click **Clear** or **Delete**, depending on your system.
4. Select **Enter** to save your changes.

Deleting pickup groups

About this task

Before deleting a pickup group, you must verify if the pickup group is a member of any simple or flexible extended pickup group. If so, you must first delete the pickup group from all extended pickup groups.

Follow these three steps to delete a pickup group:

- Get a list of all extended pickup groups.
- Verify and delete the pickup group from all extended pickup groups.
- Delete the pickup group.

Getting a list of extended pickup groups

Procedure

1. Enter `list extended-pickup-group`.
2. Print this screen or write down the existing Group Numbers so that you can check each extended pickup group.
3. Click **Cancel**.

Removing a pickup group from an extended pickup group

About this task

You must remove the pickup group from all extended pickup groups.

- If your system is set up for simple extended pickup groups, the pickup group can be a member of only one extended pickup group.
- If your system is set up for flexible extended pickup groups, the pickup group can be a member of many extended pickup groups.
- If your system is set up for no extended pickup groups (none) or has no extended pickup groups assigned, you can skip this section and see *Deleting a pickup group*.

Procedure

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

   The system displays the Extended Pickup Group screen.
3. Perform one of the following actions:
   - If the pickup group that you want to delete is not a member of this extended pickup group, Click **Cancel**.
   - If the pickup group that you want to delete is a member of this extended pickup group:
     - Select the pickup group.

- Click **Clear** or **Delete**, depending on your system.
- Click **Enter** to save your changes.

4. Repeat this procedure for each extended pickup group.

Deleting pickup groups

About this task

Before deleting a pickup group, you must verify if the pickup group is a member of any simple or flexible extended pickup group. If so, you must first delete the pickup group from all extended pickup groups.

Follow these three steps to delete a pickup group:

- Get a list of all extended pickup groups.
- Verify and delete the pickup group from all extended pickup groups.
- Delete the pickup group.

Getting a list of extended pickup groups

Procedure

1. Enter `list extended-pickup-group`.
2. Print this screen or write down the existing Group Numbers so that you can check each extended pickup group.
3. Click **Cancel**.

Removing a pickup group from an extended pickup group

About this task

You must remove the pickup group from all extended pickup groups.

- If your system is set up for simple extended pickup groups, the pickup group can be a member of only one extended pickup group.
- If your system is set up for flexible extended pickup groups, the pickup group can be a member of many extended pickup groups.
- If your system is set up for no extended pickup groups (none) or has no extended pickup groups assigned, you can skip this section and see *Deleting a pickup group*.

Procedure

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

   The system displays the Extended Pickup Group screen.
3. Perform one of the following actions:
   - If the pickup group that you want to delete is not a member of this extended pickup group, Click **Cancel**.

- If the pickup group that you want to delete is a member of this extended pickup group:
  - Select the pickup group.
  - Click **Clear** or **Delete**, depending on your system.
  - Click **Enter** to save your changes.

4. Repeat this procedure for each extended pickup group.

Deleting a pickup group

Procedure

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

   The system displays the Pickup Group screen.
3. Click **Enter**.

   The system deletes the pickup group.

Related links

Simple extended pickup groups on page 237
Flexible Extended Pickup Groups on page 239

Changing a Call Pickup button on a user telephone

Procedure

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

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

Removing a Call Pickup button from a user telephone

Procedure

1. Enter `change station n`, where *n* is the extension that you want to change.
2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
3. Move to the existing **call-pkup** button.

4. Click **Clear** or **Delete**, depending on your system.
5. Select **Enter** to save your changes.

Simple extended pickup groups

What if you want to have members in one pickup group be able to answer calls for another pickup group? In our example, what if you want members in the Credit Services pickup group 13 to answer calls in the Delinquency Payments pickup group 14? You can do that by setting up extended pickup groups.

If you want members of pickup group 13 to answer calls for pickup group 14, and if you want members of pickup group 14 to answer calls for pickup group 13, set your system for simple extended pickup groups.

Members of two or more individual pickup groups can answer each others calls using simple extended pickup groups. In a simple extended pickup group, an individual pickup group can be assigned to only one extended pickup group.

All members of one pickup group can answer the calls to the other pickup groups within the simple extended pickup group.

Caution:

Before you administer what type of extended pickup group to use (none, simple, or flexible), be sure that your pickup group objectives are well thought out and defined.

In this exercise, you will:

- Set up the system for simple extended pickup groups.
- Assign a FAC so that users can answer calls.
- Add pickup groups, if needed
- Assign two pickup groups to an extended pickup group.

Related links

Adding Pickup Groups on page 231
Deleting a pickup group on page 236

Creating simple extended pickup groups

Procedure

1. Enter `change system-parameters features`.
2. Click **Next** until you see the **Extended Group Call Pickup** field.
3. In the **Extended Group Call Pickup** field, type `simple`.
4. Select `Enter` to save your changes.

Creating an extended pickup group feature access code

About this task

Users in an extended pickup group must dial an assigned FAC, followed by a 1-digit or 2-digit Pickup Numbers, to answer calls to an extension in another pickup group. Pickup groups must be in the same extended pickup group. Users cannot use a call pickup button with Extended Call Pickup.

Procedure

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

   The system displays the Feature Access Code (FAC) screen.
3. Click **Next** until you see the **Extended Group Call Pickup Access Code** field.
4. Perform one of the following actions:
   - If the **Extended Group Call Pickup Access Code** field contains a FAC, click **Cancel**.
   - If the **Extended Group Call Pickup Access Code** field does not contain a FAC:
     - Type the required FAC.

       Make sure that the FAC complies with your dial plan.
     - Click **Enter** to save your changes.
5. Communicate the FAC, the list of pickup numbers, and the pickup group to which each pickup number is associated, to each pickup group member who is part of the extended pickup group.

Assigning pickup groups to a simple extended pickup group

Procedure

1. Type change extended-pickup-group n, where n is a number of the extended pickup group. In this example, type change extended-pickup-group 4.
2. Press `Enter`.

   The system displays the Extended Pickup Group screen for extended pickup group 4
3. In the Pickup Group Number column, type the numbers of the pickup groups that you want to link together. In this example, add pickup group 13 (Credit Services) and pickup group 14 (Delinquency Payments).
4. Press Enter to save your changes.

Example

Pickup groups 13 and 14 are now linked together in extended pickup group 4. In addition to answering calls to their own pickup group:

- All members of pickup group 13 can answer calls to pickup group 14.
- All members of pickup group 14 can answer calls to pickup group 13.

Pickup Numbers

The **Pickup Number** column that is associated with the Pickup Group Number is the unique number that users must dial after dialing the Extended Group Call Pickup Access Code FAC to answer a call in that pickup group.

For example, let us say that the Extended Group Call Pickup Access Code FAC is *39. In the above example:

- A user in pickup group 13 must dial *391 to answer a call to pickup group 14, because pickup group 14 is assigned to Pickup Number 1.
- A user in pickup group 14 must dial *390 to answer a call to pickup group 13, because pickup group 13 is assigned to Pickup Number 0.

Note:

To minimize the number of digits that a user has to dial, first assign pickup groups to Pickup Numbers 0 to 9.

- By assigning Pickup Numbers 0 to 9, all users only needs to dial a single digit (0 to 9) after the FAC to answer the call.
- If you assign a number greater than 9 (10 to 24) to any pickup group, all users must dial two digits (00 to 24) after the FAC to answer the call.

Flexible Extended Pickup Groups

If you want members of a pickup group to answer calls for another pickup group, but you do not want the other pickup group to answer your calls, set your system for flexible extended pickup groups.

Members of one or more individual pickup groups can answer calls of another pickup group using flexible extended pickup groups. However, the reverse scenario is not always true. With flexible extended pickup groups, you can prevent members of one or more pickup groups from answering the calls to another pickup group.

Flexible extended pickup groups allows more control over what pickup groups can answer calls for other pickup groups. Unlike simple extended pickup groups, an individual pickup group can be in multiple flexible extended pickup groups.

The system displays the **Extended Group Number** field on the Pickup Group screen only when you set the **Extended Group Call Pickup** field on the Feature-Related System Parameters screen to flexible. When you populate the **Extended Group Number** field on the Pickup Group screen, you are associating, or "pointing," that pickup group to an extended pickup group. By pointing to an extended pickup group, members of the pickup group can answer calls made to any member of that extended pickup group.

A specific pickup group does not have to be a member of the extended pickup group that the pickup group points to. To help clarify flexible extended pickup groups, see the Example in this section.

Caution:

Before you administer what type of extended pickup group to use (none, simple, or flexible), be sure that your pickup group objectives are well thought out and defined.

In this exercise, you will:

- Set up the system for flexible extended pickup groups.
- Assign a FAC so that users can answer calls.
- Add or change pickup groups, and "point" a pickup group to an extended pickup group.

Related links

Adding Pickup Groups on page 231
Deleting a pickup group on page 236

Creating flexible extended pickup groups

Procedure

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

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

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

   To create an extended pickup group FAC, see *Creating an extended pickup group feature access code*.

Associating individual pickup groups with an extended pickup group

Procedure

1. Type `change pickup-group n`, where `n` is a pickup group number.

   In this example, let us change pickup group 15 (Executives). Type change `pickup-group 15`.
2. Press `Enter`.

   The system displays the Pickup Group screen. Notice that the system displays the **Extended Group Number** field on the Pickup Group screen. The system will display this field because you set the **Extended Group Call Pickup** field on the Feature-Related System Parameters screen to flexible.

   Important:

   If you change your system from simple to flexible extended pickup groups (see *Changing extended pickup groups*), the system automatically populates the **Extended**

Group Number field on the Pickup Group screen for each pickup group member. For example, pickup groups 13 and 14 are members of extended pickup group 4. If you change the system from simple to flexible extended pickup groups, the system automatically populates the **Extended Group Number** field to 4 on the Pickup Group screen for these two pickup groups.

You are not required to keep the number that the system automatically populates in the **Extended Group Number** field. You can change the number in the **Extended Group Number** field to another pickup group number. You can also make the field blank.

3. If you want to associate, or "point" the pickup group to an extended pickup group, type the number of the extended pickup group for which this pickup group can answer calls in the **Extended Group Number** field. In this example, manually associate pickup group 15 (Executives) to extended pickup group 4. For this example, let us say that you followed the same procedure for pickup group 16 (Finance).

   Note:

   You do not have to populate the **Extended Group Number** field. You can leave the **Extended Group Number** field blank. You can just as easily point the pickup group to a different extended pickup group. For example, you can point pickup group 13 (Credit Services) to extended pickup group 2, even though pickup group 13 is not a member of extended pickup group 2.

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

Assigning pickup groups to a flexible extended pickup group

Procedure

1. Type `change extended-pickup-group n`, where `n` is the number of the extended pickup group.

   In this example, type `change extended-pickup-group`.

2. Press `Enter`.

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

3. Add pickup group 16 (Finance) to this extended pickup group.
4. Click **Enter** to save your changes.

Example

Here is how flexible extended pickup groups work.

Notice that pickup groups 13, 14, and 16 are now members of extended pickup group 4. On the Pickup Group screen for pickup groups 13, 14, and 16, you also pointed each pickup group to extended pickup group 4.

Pickup group 15 (Executives) is not a member of extended pickup group 4. However, on the Pickup Group screen for group 15 (Figure 96: Pickup Group screen on page 266), you pointed pickup group 15 to extended pickup group 4.

In addition to answering calls to their own pickup group:

Notice that pickup groups 13, 14, and 16 are now members of extended pickup group 4. On the Pickup Group screen for pickup groups 13, 14, and 16, you also pointed each pickup group to extended pickup group 4.

Pickup group 15 (Executives) is not a member of extended pickup group 4. However, on the Pickup Group screen for group 15 (Figure 96), you pointed pickup group 15 to extended pickup group 4.

In addition to answering calls to their own pickup group:

- Any member of pickup group 13 can answer calls to pickup groups 14 and 16.
- Any member of pickup group 14 can answer calls to pickup groups 13 and 16.
- Any member of pickup group 16 can answer calls to pickup groups 13 and 14.
- Any member of pickup group 15 can answer calls to pickup groups 13, 14, and 16 because pickup group 15 points to extended pickup group 4.
- Any member of pickup groups 13, 14 and 16 cannot answer calls to pickup group 15 because pickup group 15 is not a member of extended pickup group 4.

Changing extended pickup groups

About this task

You define extended pickup groups on a system-wide basis. The system cannot support both simple and flexible extended pickup groups at the same time. You can, however, change your extended pickup groups from one type to another.

Related links

Call Pickup on page 228
Simple extended pickup groups on page 237
Flexible Extended Pickup Groups on page 239
Directed Call Pickup on page 243

Changing from simple to flexible

About this task

If you want to change all extended pickup groups from simple to flexible, you can easily make the change. See *Creating flexible extended pickup groups*. The system automatically populates the **Extended Group Number** field on the Pickup Group screen for all pickup groups that are part of an extended pickup group.

Changing from flexible to simple

About this task

The process is more complex to change all extended pickup groups from flexible to simple. Before you can change the extended pickup group from flexible to simple, you must first delete all of the individual pickup groups from all of the extended pickup groups. Then you can change the extended pickup group from flexible to simple (see *Creating simple extended pickup groups*). After that step, you must re-administer all of the extended pickup groups again.

Directed Call Pickup

If you do not want to set up pickup groups and extended pickup groups, but still want selected people to answer other telephones, use Directed Call Pickup. Before a person can use this feature, you must enable Directed Call Pickup on your system.

- Telephones that can be answered by another extension using Directed Call Pickup must have a Class of Restriction (COR) that allows this feature.
- Telephones that can answer another extension using Directed Call Pickup must have a COR that allows this feature.

In this exercise, you will:

- Determine if Directed Call Pickup is enabled on your system.
- Create one or more Classes of Restriction (COR) that allow Directed Call Pickup.
- Assign the COR to individual extensions.
- Assign a Directed Call Pickup button to each extension that is assigned the COR.
- Assign a feature access code (FAC).

Ensuring Directed Call Pickup availability

About this task

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

Procedure

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

   The system displays the Feature-Related System Parameters screen.
3. Click **Next** until you see the **Directed Call Pickup?** field
4. Perform one of the following actions:
   a. If the **Directed Call Pickup?** field is set to y, your system is set up for Directed Call Pickup. Click **Cancel**.
   b. If the **Directed Call Pickup?** field is set to n:
      - Type `y` in the field.
      - Click **Enter** to save your changes.

Creating Classes of Restriction for Directed Call Pickup

About this task

You must create one or more Classes of Restriction (COR) for Directed Call Pickup. All users to whom you assign a COR can then use Directed Call Pickup.

There are three ways to set up a COR for Directed Call Pickup. You can create a COR where users can:

- Only have their extensions answered by Directed Call Pickup. Users with this COR cannot pick up other extensions.
- Only pick up other extensions using Directed Call Pickup. Users with this COR cannot have their extensions answered by other users.
- Both have their extensions answered by Directed Call Pickup and pick up other extensions.

Procedure

1. Enter `change COR n`, where *n* is the COR that you want to change.
2. Perform one of the following actions:
   a. To create one or more CORs where the extensions can only be picked up by the Directed Call Pickup feature, but unable to pick up other extensions:
      - Type `y` in the **Can Be Picked Up By Directed Call Pickup** field.
      - Leave the **Can Use Directed Call Pickup** field set to `n`.

        Any extension to which you assign this COR can only be picked up by the Directed Call Pickup feature.

   b. To create one or more CORs where the extensions can only use the Directed Call Pickup feature to pick up other extensions, but not be picked up by other extensions:
      - Leave the **Can Be Picked Up By Directed Call Pickup** field set to `n`.
      - Type `y` in the **Can Use Directed Call Pickup** field.

        Any extension to which you assign this COR can only use the Directed Call Pickup feature to pick up other extensions.

   c. To create one or more CORs where the extensions can use the Directed Call Pickup feature both to pick up other extensions and be picked up by other extensions:
      - Type `y` in the **Can Be Picked Up By Directed Call Pickup** field.
      - Type `y` in the **Can Use Directed Call Pickup** field.

        Any extension to which you assign this COR can use the Directed Call Pickup feature both to pick up other extensions and be picked up by other extensions.
3. Select **Enter** to save your changes.

Assigning a Class of Restriction to a user

About this task

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

Procedure

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

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

Assigning a Directed Call Pickup button

About this task

Assign a Directed Call Pickup button to all extensions that share a COR where the **Can Use Directed Call Pickup** field is set to y.

Procedure

1. Enter `change station n`, where *n* is an extension to which you have assigned the Directed Call Pickup COR.
2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
3. Move to the button number that you want to use for Directed Call Pickup. You can use any of the available buttons.
4. Type `dir-pkup` after the button number.
5. Select **Enter** to save your changes.

   Repeat this procedure for each member of the COR who can pick up other extensions using Directed Call Pickup.

Assigning a Directed Call Pickup feature access code

About this task

Also assign a Directed Call Pickup feature access code (FAC). Give the FAC to each user whose extension shares a **COR where the Can Use Directed Call Pickup** field is set to y.

Instead of using the Directed Call Pickup button, users can dial the assigned FAC to answer calls using Directed Call Pickup.

Procedure

1. Enter `change feature-access-codes`.
2. Click **Next** until you see the **Directed Call Pickup Access Code** field.
3. Perform one of the following actions:
   a. If the **Directed Call Pickup Access Code** field already contains a code, click **Cancel**.
   b. If the **Directed Call Pickup Access Code** field does not contain a code:
      - Type a code in the field. Make sure that the code you type conforms to your dial plan.
      - Select **Enter** to save your change.

   Communicate the FAC with each member of the COR that can pick up other extensions using Directed Call Pickup.

Removing Directed Call Pickup from a user

Procedure

1. Enter `change station n`, where *n* is the extension of the user.
2. In the **COR** field, type a different COR that does not have Directed Call Pickup permissions.
3. Click **Next** until you see the **BUTTON ASSIGNMENTS** section.
4. Move to the button number that contains dir-pkup.
5. Click **Clear** or **Delete**, depending on your system.
6. Select **Enter** to save your changes.

Hunt Groups

A hunt group is a group of extensions that receive calls according to the call distribution method you choose. When a call is made to a certain telephone number, the system connects the call to an extension in the group.

Use hunt groups when you want more than one person to be able to answer calls to the same number. For example, set up a hunt group for:

- a benefits department within your company
- a travel reservations service

Setting up hunt groups

About this task

Let us set up a hunt group for an internal helpline. Before making changes to Communication Manager, we will decide:

- the telephone number for the hunt group
- the number of people answering calls
- the way calls are answered

Our dial plan accepts 4-digit internal numbers that begin with 1. The number 1200 is not in use. So, we'll set up a helpline hunt group so anyone within the company can call extension 1200 for help with a telephone.

We will assign 3 people (agents) and their extensions to our helpline. We want calls to go to the first available person.

Procedure

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

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

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

   In our example, type `internal helpline`.

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

   We'll type `1200`.

5. In the **Group Type** field, type the code for the call distribution method you choose.

   We'll type `ucd-loa` so a call goes to the agent with the lowest percentage of work time since login.

   Note:

   The COS for all hunt groups defaults to 1. Therefore, any changes to COS 1 on the Class of Service screen changes the COS for all your hunt groups. A **COS** field does not appear on the Hunt Group screen.

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

7. In the **Ext** field, type the extensions of the agents you want in the hunt group.

   We'll type `1011`, `1012`, and `1013`.

   Tip:

   For a ddc group type (also known as "hot seat" selection), the call is sent to the extension listed in the first **Ext** field. The system uses this screen to determine the hunting sequence.

8. Click **Enter** to save your changes.

   The **Name** fields are display-only and do not appear until the next time you access this hunt group.

Dynamic hunt group queue slot allocation

The dynamic hunt group queue slot allocation feature eliminates the need to preallocate queue slots for hunt groups. The system dynamically allocates the queue slots from a common pool on an as-needed basis. All possible calls can be queued. There is no additional administration needed. This feature expands the capacities of your system by eliminating the potential of missed calls due to a full queue

When the **Queue?** field on the Hunt Group screen is set to y, this feature applies to all uses of hunt groups:

- Automatic Call Distribution (ACD) non-vector/vector splits and skills
- Non-ACD hunt group
- Voice mail

Changing a hunt group

Procedure

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

Setting up a queue

About this task

You can tell your server running Communication Manager how to handle a hunt-group call when it cannot be answered right away. The call waits in "queue."

We will tell Communication Manager that as many as 10 calls can wait in the queue, but that you want to be notified if a call waits for more than 30 seconds.

You also want Communication Manager to send a warning when 5 or more calls are waiting in the queue. This warning flashes queue-status buttons on telephones that have a status button for this hunt group. When the buttons flash, everyone answering these calls can see that the help-line calls need more attention.

Procedure

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

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

   The system displays the Hunt Group screen.
3. In the **Queue** field, type `y`.
4. In the **Queue Length** field, type the maximum number of calls that you want to wait in the queue.

   In our example, type `10`.
5. In the **Calls Waiting Threshold** field, type the maximum number of calls that can be in the queue before the system flashes the queue status buttons.

   In our example, type `5`.
6. In the **Time Warning Threshold** field, type the maximum number of seconds you want a call to wait in the queue before the system flashes the queue status buttons.

   In our example, type `30`.
7. Click **Enter** to save your changes.

Hunt groups for TTY callers

Several laws, such as the Americans with Disabilities Act (ADA) of 1990 and Section 255 of the Telecommunications Act of 1996, require that“ reasonable accommodation” be provided for people with disabilities. For this reason, your company might choose to offer support for callers who use TTYs. (These devices are also known as TDDs -- “Telecommunication Device for the Deaf” -- but the term TTY is generally preferred, in part because many users of these devices are hearing-impaired, but not deaf.)

TTY callers can be accommodated by creating a hunt group that includes TTY-equipped agents. The TTY itself looks a little like a laptop computer, except that it has a one- or two-line alphanumeric display instead of a computer screen. The cost of a typical TTY is approximately three hundred dollars. Although many TTYs can connect directly with the telephone network via analog RJ-11 jacks, Avaya recommends that agents be equipped with TTYs that include an acoustic coupler that can accommodate a standard telephone handset. One reason for this recommendation is that a large proportion of TTY users are hearing impaired, but still speak clearly. These individuals often prefer to receive calls on their TTYs and then speak in response. This requires the call center agent to alternate between listening on the telephone and then typing on the TTY, a process made considerably easier with an acoustically coupled configuration.

Although TTY-emulation software packages are available for Personal Computers, most of these do not have the ability to intermix voice and TTY on the same call.

For a TTY hunt group, you can record TTY announcements and use them for the hunt group queue. To record announcements for TTY, simply follow the same steps as with voice recordings from your telephone (see *Managing Announcements*). However, instead of speaking into your telephone to record, you type the announcement with the TTY device.

Note:

For an alternative to simply creating a TTY hunt group, you can use vectors to process TTY calls. With vectors, you can allow TTY callers and voice callers to use the same telephone number. In this case, you can also record a single announcement that contains both TTY signaling and a voice recording.

Adding hunt group announcements

About this task

You can add recorded announcements to a hunt group queue. Use announcements to encourage callers to stay on the line or to provide callers with information. You can define how long a call remains in the queue before the caller hears an announcement.

For more information on how to record an announcement, see “Announcements” in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Let us add an announcement to our internal helpline. We want the caller to hear an announcement after 20 seconds in the queue, or after approximately 4 or 5 rings. Our announcement is already recorded and assigned to extension 1234.

Tip:

You can use `display announcements` to find the extensions of your recorded announcements.

Procedure

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

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

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

   In this example, type `1234`.
5. In the **First Announcement Delay (sec)** field, type the number of seconds you want the caller to wait before hearing the first announcement.

   In our example, type `20`.

   Tip:

   If you set the delay announcement interval to 0, callers automatically hear the announcement before anything else. This is called a “forced first announcement.”
6. Click **Enter** to save your changes.

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

Vectors and VDNs

This section provides an introduction to vectors and Vector Directory Numbers (VDN). It gives you basic instructions for writing simple vectors.

Security alert:

Vector fraud is one of the most common types of toll fraud because vectors route calls based on the Class of Restriction (COR) assigned to the VDN.

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 Elite Feature Reference*.

Note:

The **Client Room** field on the Class of Service screen will affect VDN displays. If a local station that has a COS with the **Client Room** field set to y calls a local VDN, the agent's display that receives the call will look as if it is a direct station call rather than the expected VDN display of station name to vdn name.

What are Vectors?

A vector is a series of commands that you design to tell the system how to handle incoming calls. A vector can contain up to 32 steps and allows customized and personalized call routing and treatment. Use call vectoring to:

- play multiple announcements
- route calls to internal and external destinations
- collect and respond to dialed information

Tip:

The vector follows the commands in each step in order. The vector "reads" the step and follows the command if the conditions are correct. If the command cannot be followed, the vector skips the step and reads the next step.

Your system can handle calls based on a number of conditions, including the number of calls in a queue, how long a call has been waiting, the time of day, day of the week, and changes in call traffic or staffing conditions.

Putting a call in a queue

About this task

Write a vector so that calls that come into the main business number redirect to a queue.

We will use a vector-controlled hunt group for the main number queue. This hunt group was set up as main split 47. When calls first arrive, all calls to our main number should be queued as “pri 1” for low priority.

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

Procedure

1. Keep it Blank.
2. Type `queue-to main split 47 pri 1`.

   Tip:

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

Playing an Announcement

About this task

Write a vector to play an announcement for callers in a queue. Use the announcement to ask callers to wait. You need to record the announcement before the vector can use it.

Let us play our announcement 4001, asking the caller to wait, then play music for 60 seconds, then repeat the announcement and music until the call is answered. The goto command creates the loop to repeat the announcement and the music. Unconditionally means under all conditions.

Tip:

Rather than loop your vectors directly back to the announcement step, go to the previous queue-to step. This way, if for some reason the call does not queue the first time, Communication Manager can attempt to queue the call again. If the call successfully queued the first time though, it merely skips the queue-to step and plays the announcement. The system cannot queue a call more than once in the exact same priority level.

To play and repeat an announcement, write this vector (steps 3-5):

Procedure

1. Keep it Blank.
2. Type `queue-to main split 47 pri 1.`
3. Type `announcement 4001 (All agents are busy, please wait...).`
4. Type `wait-time 60 secs hearing music.`
5. Type `goto step 2 if unconditionally.`

Routing Based On Time Of Day

About this task

Write a vector for calls that come in after your office closes.

Assume that your business is open 7 days a week, from 8:00 a.m. to 5:00 p.m. When calls come in after business hours, you want to play your announcement 4002, which states that the office is closed and asks callers to call back during normal hours. Write the vector so the call disconnects after the announcement is played.

For after hours treatment, write this vector (steps 1, 6, and 7):

Procedure

1. Type `goto step 7 if time-of-day is all 17:00 to all 8:00.`
2. Type `queue-to main split 47 pri 1.`
3. Type `announcement 4001 (All agents are busy, please wait...).`
4. Type `wait-time 60 secs hearing music.`
5. Type `goto step 2 if unconditionally.`
6. Type `stop.`

7. Type `disconnect after announcement 4002 ("We're sorry, our office is closed...")`.

   If the `goto` command in step 5 fails, Communication Manager goes to the next step. The `stop` in step 6 prevents callers from incorrectly hearing the "office is closed" announcement in step 7. `Stop` keeps the call in the state it was in before the command failed. In this case, if step 5 fails, the call remains in step 4 and the caller continues to hear music.

   Caution:

   Add a stop vector step only after calls are routed to a queue. If a stop vector is executed for a call not in queue, the call drops.

Allowing callers to leave a message

About this task

Write a vector using which callers can leave messages. This type of vector uses a hunt group called a messaging split. For our example, we send after-hours calls to the voice mailbox at extension 2000 and use messaging split 99.

Once the vector routes a call to the mailbox, the caller hears a greeting (that was recorded with the voice mail for mailbox 2000) that tells them they can leave a message.

To let callers leave messages, write this vector (step 7):

Procedure

1. Type `goto step 7 if time-of-day is all 17:00 to all 8:00`.
2. Type `queue-to main split 47 pri 1`.
3. Type `announcement 4001 (All agents are busy, please wait...)`.
4. Type `wait-time 60 secs hearing music`.
5. Type `goto step 2 if unconditionally`.
6. Type `stop`.
7. Type `messaging split 99 for extension 2000`.

Redirecting calls during an emergency or holiday

About this task

You can provide a quick way for a supervisor or agent to redirect calls during an emergency or holiday. Use a special mailbox where you can easily change announcements. This vector is also an alternative to making sure all agents log out before leaving their telephones.

In our example, no agents are normally logged in to split 10. We'll use split 10 for an emergency. We preset buttons on our agents' telephones so people with these telephones can log in at the touch of a button.

To quickly redirect calls:

Create a special mailbox with the appropriate announcement such as “We are unable to answer your call at this time” or ""Today is a holiday, please call back tomorrow.”

In our example, we recorded the mailbox greeting for extension 2001.

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

See *Inserting a step*.

Procedure

1. Type `goto step 10 if staff agents split 10 > 0.`
2. Type `goto step 8 if time-of-day is all 17:00 to all 8:00.`
3. Type `queue-to main split 47 pri 1.`
4. Type `announcement 4001 (All agents are busy, please wait...).`
5. Type `wait-time 60 secs hearing music.`
6. Type `goto step 2 if unconditionally.`
7. Type `stop.`
8. Type `messaging split 99 for extension 2000.`
9. Type `stop.`
10. Type `messaging split 99 for extension 2001.`
11. Type `stop.`

    When there is an emergency, fire drill, or holiday, the supervisor or agent logs into this split. When an agent logs into split 10, the system looks at vector step 1, sees that more than 0 people are logged into split 10, and sends calls to step 10 (which sends to messaging split 99). When your business returns to normal and the agent logs out of split 10, call handling returns to normal.

Giving callers additional choices

About this task

You can give your callers a list of options when they call. Your vector tells Communication Manager to play an announcement that contains the choices. Communication Manager collects the digits the caller dials in response to the announcement and routes the call accordingly.

We’ll create a vector that plays an announcement, then lets callers dial an extension or wait in the queue for an attendant.

Please note, the following example of this “auto attendant” vector is a new vector and is not built on the vector we used in the previous example.

To let callers connect to an extension, write this kind of vector:

Procedure

1. Type `wait-time 0 seconds hearing music.`

2. Type `collect 4 digits after announcement 4004 (You have reached our company. Please dial a 4-digit extension or wait for the attendant.)`.
3. Type `route-to digits with coverage y`.
4. Type `route-to number 0 with cov n if unconditionally`.
5. Type `stop`.

Inserting a Step

About this task

It is easy to change a vector step and not have to retype the entire vector. We will add announcement 4005 between step 3 and step 4 in vector 20.

Procedure

1. Type `change vector 20`. Press `Enter`.

   The system displays the Call Vector screen.
2. Click **Edit**.
3. Type `i` followed by a space and the number of the step you want to add.

   In our example, type `i 4`.
4. Type the new vector step.

   We will type `announcement 4005 (Please wait...)`.
5. Click **Enter** to save your changes.

   Tip:

   When you insert a new vector step, the system automatically renumbers the rest of the vector steps and all references to the vector steps. Communication Manager inserts a "*" when the numbering needs more attention.

Deleting a Step

Procedure

1. Type `change vector 20`. Press `Enter`.

   The system displays the Call Vector screen.
2. Click **Edit**.
3. Type `d` followed by a space and the number of the step you want to delete.

   In our example, type `d 5`.

Tip:

You can delete a range of vector steps. For example, to delete steps 2 through 5, type `d 2-5`. Click **Enter**.

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

Tip:

When you delete a vector step, the system automatically renumbers the rest of the vector steps and all references to the vector steps. An asterisk (*) is inserted when the numbering needs more attention.

Variables in Vectors

You can use Call Vectoring feature called Variables in Vectors (VIV) 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
- Create more flexible vectors that serve the needs of your customer and contact center operations

The vector variables are defined in a central variable administration table. Values assigned to some types of variables can also be quickly changed by means of special vectors, Vector Directory Numbers (VDNs), or Feature Access Codes (FACs) that you administer specifically for that purpose. Different types of variables are available to meet different types of call processing needs. Vector variables can be added to “consider location,”“messaging,” and ""adjunct routing” vector steps when the Call Center Release is 3.0 or later. Depending on the variable type, variables can use either call-specific data or fixed values that are identical for all calls. In either case, an administered variable can be reused in many vectors. For a more detailed description of variable types and purposes, see *Avaya Call Center Call Vectoring and Expert Agent Selection (EAS) Guide, 07-600780*.

Administering Vector Variables

About this task

Administering variables and implementing them in your vectors is a relatively simple process:

Procedure

1. First, determine how you intend to use the new variable and identify its defining characteristics. Use this information to decide on an available variable type that meets your needs.
2. Type `change variables`.

   The 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. Click **Enter** to save your changes.

Handling TTY calls with vectors

About this task

Unlike fax machines and computer modems, a Tele-typewriter device (TTY) has no handshake tone and no carrier tone. A TTY is silent when not transmitting. This is why systems cannot identify TTY callers automatically. However, the absence of these special tones also means that voice and TTY tones can be intermixed in pre-recorded announcements. The ability to provide a hybrid voice-and-TTY announcement, when combined with the auto-attendant vectoring capability, can permit a single telephone number to accommodate both voice and TTY callers.

With the sample vector TTY callers can access a TTY agent. It begins with a step that plays a TTY announcement combined with a voice announcement. The announcement tells the TTY caller to enter a digit that will direct them to a TTY support person. The vector then processes the digit entered to connect the TTY caller to the TTY split (or hunt group). For more information on recording TTY announcements, see *Managing Announcements*.

In the following example, split 47 (hunt group 47) has already been established and consists of TTY-enabled agents.

If a TTY caller calls the number that connects to vector 33, the following occurs:

Procedure

1. After a short burst of ringing, a quick burst of TTY tones is sent to the caller telling the caller to hold, “HD”. Then, a voice announcement follows for callers using a normal telephone connection. The announcement tells them to stay on the line. Finally, another burst of TTY tones is sent to the TTY caller which displays on the caller’s TTY device as,“Dial 1.” The TTY caller would not hear the voice announcement, but because the step collects digits, using which the caller can enter `1` on his or her touchtone telephone.

   Note:

   For voice callers, the burst of TTY tones lasts about one second and sounds like a bird chirping.

2. In vector step 3, since the TTY caller entered `1` in vector step 2, the TTY caller is sent to vector step 8, at which point the caller is put in queue for a TTY-enabled agent in split 47.

Note:

The voice caller is sent to vector step 3 also, but a voice caller does not go to vector step 8 because the caller did not enter `1` at vector step 2. Instead, voice callers continue on to vector step 4, where they connect to split 48.

3. While the TTY caller waits in queue, he or she hears silence from vector step 9, then the announcement in vector step 10, and is then looped back to wait with silence by vector step 11.

   See the *Avaya Call Center Call Vectoring and Expert Agent Selection (EAS) Guide, 07-600780*, for more information.

   Automated Attendant competes with several features for ports on the Call Classifier — Detector circuit pack or equivalent. For more information on circuit pack, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Fixing vector problems

About this task

If there is a problem with a vector, Communication Manager records the error as a vector event. Vector events occur for a number of reasons including problems with a trunk, full queue slots, or the vector reaching the maximum 1000 steps allowed.

Use `display events` to access the Event Report screen and see the event record. Use the event record to see why the vector failed.

To view the Event Report:

Procedure

1. Type `display events`.
2. Press `Enter`.

   The system displays the Event Report screen.

3. To see all current vector events, click**Enter**.

   OR

   Indicate the events that you want to see by completing the **Report Period** and **Search Option** fields.

4. Click **Enter** to view the report.

   The system displays the Event Report (detail) screen.

   Look at the information in the **Event Data** field to diagnose the vector event. In this example, there was a problem with:

   - Vector 12, step 5
   - Split 89

Vector Directory Numbers

A VDN is an extension that directs an incoming call to a specific vector. This number is a “soft” extension number not assigned to an equipment location. VDNs must follow your dial plan.

We will create VDN 5011 for our sales department. A call into 5011 routes to vector 11. This vector plays an announcement and queues calls to the sales department.

Security alert:

Vector fraud is one of the most common types of toll fraud because vectors route calls based on the class of restriction (COR) assigned to the VDN. See the *Avaya Toll Fraud and Security Handbook*, 555-025-600 for more information.

Adding a vector directory number

Procedure

1. Type `add VDN 5011`.
2. Press `Enter`.
3. You enter the VDN extension you want to add.

   The system displays the Vector Directory Number screen.
4. Type a description for this VDN in the **Name** field.

   In our example, type `Sales Department`.

   The system displays the information in the VDN **Name** field on a display telephone. The agent uses this to recognize the nature of the call and respond accordingly.

   Tip:

   The **VDN Override** on the Vector Directory Number screen controls the operation of the display.
5. Enter the vector number.

   In our example, type `11`.
6. In the **Measured** field, indicate how you want to measure calls to his VDN.

   In our example, type `both` (for both CMS and BCMS).

   Tip:

   BCMS must be enabled to use both. Use `display system-parameters customer-options` to see if BCMS is enabled.
7. Click **Enter** to save your changes.

Viewing vector directory numbers

Procedure

1. Type `list VDN`.
2. Press `Enter`.

   The system displays the Vector Directory Number screen.
3. Each VDN maps to one vector. Several VDNs can map to the same vector.

Automatic Call Distribution

Automatic Call Distribution (ACD) is an Avaya Communication Manager feature used in many contact centers. ACD gives you greater flexibility to control call flow and to measure the performance of agents.

ACD systems operate differently from non-ACD systems, and they can be much more complex. ACD systems can also be more powerful because using this you can use features and products that are unavailable in non-ACD systems. See the *Avaya Call Center Release 4.0 Automatic Call Distribution (ACD) Guide, 07-600779*, for more information on ACD call centers.

ACD System Enhancement

First, all call center management systems (such as Avaya's Basic Call Management System (BCMS), BCMSVu, and the sophisticated Avaya IP Agent Call Management System) require ACD. These management systems give you the ability to measure more aspects of your center's operation, and in more detail, than is possible with standard Avaya Communication Manager reports.

Call vectoring greatly enhances the flexibility of a call center, and most vectoring functions require ACD. Vectoring is a simple programming language using which you can custom design every aspect of call processing.

With ACD and Vectoring, you can 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.

Using EAS you can classify agents according to their specific skills and then to rank them by ability or experience within each skill. Avaya Communication Manager uses these classifications to match each call with the best available agent. See *Avaya Call Center Call Vectoring and Expert Agent Selection (EAS) Guide, 07-600780*, for more information on call vectoring and EAS.

Assigning a Terminating Extension Group

About this task

A Terminating Extension Group (TEG) allows an incoming call to ring as many as 4 telephones at one time. Any user in the group can answer the call.

Once a member of the TEG has answered a group call, the TEG is considered busy. If a second call is directed to the group, it follows a coverage path if one has been assigned.

The following example shows how to assign a terminating extension group to the advertising department.

For example, we will assign this TEG to extension 6725.

Procedure

1. Type `add term-ext-group next`.
2. Press `Enter`.

   The system displays the Terminating Extension Group screen.
3. In the **Group Extension** field, type `6725`.

   This is the extension for the advertising group.
4. In the **Group Name** field, type `advertising`.

   This is the name of the group.
5. In the **Coverage Path** field, type `5`.

   This is the number of the call coverage path for this group.

Chapter 11: Routing Outgoing Calls

World class routing

The system uses Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) to direct outgoing calls:

- AAR to route internal calls that you make within your company network.

  AAR requires a private network to route calls.

- ARS to route external calls that you make over a public network.

  ARS does not require a private network to direct outgoing calls.

  You can use ARS for remote locations of the company that do not have a private network.

Ensure that you dial a Feature Access Code (FAC) followed by the number you want to call before you begin to use automatic routing.

During automatic routing, Avaya Communication Manager does the following:

1. Analyzes the digits that you dial.
2. Selects the route for the call.
3. Deletes or inserts digits required to route the call.
4. Routes the call over the trunks that you specify in your routing tables.

ARS and AAR access the same trunk groups and share the same route patterns and information about call routing.

You can convert ARS calls to AAR calls and vice versa.

The FAC for AAR is the digit 8.

The FAC for ARS is the digit 9 within the US and the digit 0 outside the United States. You can administer your own ARS FAC.

A technician or a business partner from Avaya can help you set up Communication Manager and assign the AAR FAC.

Call Privileges Management

Each time you set up a telephone, 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 offered to 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 a user. The levels of FRL are ranked from 0 to 7 where 7 has the highest level of privileges.

On the Route Pattern screen, you can assign an FRL to each route pattern preference. The system checks the COR when the user makes a call. The system facilitates the call if the FRL of the caller is higher than or equal to the FRL of the route pattern.

Changing station

About this task

Use the following procedure to set up a new telephone for an executive and change station 1234 from COR 1 to COR 7.

The latest translations are assigned for COR 1 with outward restrictions. You must assign a COR with the highest level of permissions to station 1234.

FRL 0 is the lowest permission level.

FRL 7 is the highest permission level.

Procedure

1. On the SAT command line interface, type `change station 1234`.
2. Press **Enter**.

   The system displays the Station screen.
3. In the **COR** field, type `7`.
4. To save the changes that you make, press **Enter**.
5. To change the permission level from FRL 0 to FRL 7, type `change cor 7`.
6. Click **Enter**.

   The system displays the Class of Restriction screen.
7. In the **FRL** field, type `7`.
8. To save the changes that you make, press **Enter**.

   Users with COR 7 have the highest level of calling permissions.

Assigning ARS FAC

Before you begin

Ensure that you set up the ARS FAC on your system. The ARS FAC within the United States is the digit 9. Users dial 9 to make an outgoing call.

About this task

The ARS access code 9 is dropped when a user dials 9 to access ARS and makes an outgoing call. The ARS access code 9 is dropped before digit analysis takes place.

Procedure

1. On the SAT command line interface, type `change dialplan`.
2. Press **Enter**.

   The system displays the DCS to QSIG TSC Gateway.
3. Move to row 9 and type `fac` in the first column.
4. To save the changes that you make, press **Enter**.
5. Type `change features`.
6. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen.
7. In the **ARS - access code** field, type `9`.
8. To save the changes that you make, press **Enter**.

Location ARS FAC

Use **Location ARS FAC** to access the ARS FAC feature from different locations, and dial 9 while making external calls. For locations that you specify, use **Location ARS FAC** to call numbers administered by the ARS FAC. For more information about setting up **Location ARS FAC**, see the Locations screen.

You cannot use an ARS FAC at a location for which the ARS FAC is invalid.

The ARS access code on the Feature Access Code (FAC) screen is in use for locations where ARS FAC was previously used.

If a location has already administered the ARS FAC, the Feature Access Code (FAC) screen is denied from the location.

If you use a local ARS code, you cannot administer two ARS codes on the Feature Access Code (FAC) screen.

Displaying ARS analysis information

About this task

You will want to become familiar with how your system currently routes outgoing calls. To display the ARS Digit Analysis Table that controls how the system routes calls that begin with 1:

Procedure

1. Type `display ars analysis 1`.

2. Press **Enter**.

   The system displays the ARS Digit Analysis Table for dialed strings that begin with 1.

   Communication Manager displays only as many dialed strings as can fit on one screen at a time.

   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, Branch Gateways and Servers*.

3. To see all the dialed strings that are defined for your system, run an ARS Digit Analysis report:

   a. Type `list ars analysis`.

   b. Press **Enter**.

      The system displays the ARS Digit Analysis Report.

   To maintain a record, print a report.

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 ARS digit analysis table. Your system likely has more defined dialed strings than this example. Refer to the following screenshot for ARS Digit Analysis Table.

```
change ars analysis 1                                          Page   1 of   2
                          ARS DIGIT ANALYSIS TABLE
                                Location: all            Percent Full: 0

      Dialed          Total     Route    Call   Node  ANI
      String        Min   Max  Pattern  Type   Num   Reqd
101xxxx0            8     8    deny     op           n
101xxxx0            18    18   deny     op           n
101xxxx01           16    24   deny     iop          n
101xxxx011          17    25   30       fnpa         n
101xxxx1            18    18   deny     fnpa         n
10xxx0              6     6    deny     op           n
10xxx0              16    16   deny     op           n
10xxx01             14    22   deny     iop          n
10xxx011            15    23   deny     intl         n
10xxx1              16    16   deny     fnpa         n
3                   11    11   deny     fnpa         n
1200                11    11   deny     fnpa         n
121                 11    11   deny     fnpa         n
122                 11    11   deny     fnpa         d
123                 11    11   deny     fnpa         n
```

In the ARS Digit Analysis Table screen, the far-left column of 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 ARS Digit Analysis 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 ARS Digit Analysis Table screen.

In this example, the dialed string matches the “1”. Then Communication Manager matches the length of the entire dialed string (11 digits) to the minimum and maximum length columns. In our example, the 11-digit call that started with 1 follows route pattern 30 as an fnpa call.

Tip:

The first dialed digit for an external call is often an access code. If ‘9’ is defined as the ARS access code, Communication Manager drops this digit and analyzes the remaining digits with the ARS Analysis Table.

The Route Pattern points to the route that handles the calls that match this dial string. **Call Type** tells what kind of call is made with this dial string.

Call type helps Communication Manager decide how to handle the dialed string.

Examples of Digit Conversion

Purpose

Your system uses the AAR or ARS Digit Conversion Table to change a dialed number for more efficient routing. Digits can be inserted or deleted from the dialed number. For instance, you can tell Communication Manager to delete a 1 and an area code on calls to one of your locations, and avoid long-distance charges by routing the call over your private network.

ARS digit conversion examples

The ARS digit conversion table reflects these values:

- ARS feature access code = 9
- AAR feature access code = 8
- Private Network Office Code (also known as Home RNX) = 222
- Prefix 1 is required on all long-distance DDD calls
- Dashes (-) are for readability only

Communication Manager maps the dialed digits to the matching pattern that most closely matches the dialed number.

Example:

If the dialed string is 957-1234 and matching patterns 957-1 and 957-123 are in the table, the match is on pattern 957-123.

ARS digit conversion examples table:

Operation	Actual Digits Dialed	Matching Pattern	Replacement String	Modified Address	Notes
DDD call to ETN	9-1-303-538-1345	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).
International call to announcement (This method can also be used to block unauthorized IDDD calls)	9-011-91-672530	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-XXXXXXXX	00	+00+	00+XXXX	The first 0 denotes ARS, the second pair of 0s denotes an international call, the pluses denote “wait” for dial tone detection.

Defining operator assisted calls

About this task

Here is an example of how Communication Manager routes an ARS call that begins with 0 and requires operator assistance. The user dials 9 to access ARS, then a 0, then the rest of the number.

Procedure

1. Type `display ars analysis 0`.
2. Press **Enter** to view the AAR and ARS Digit Analysis Table screen starting with 0.

   We will use the ARS digit analysis table shown above and follow the routing for an operator assisted a call to NJ.

   We will use the ARS digit analysis table shown above and follow the routing for an operator assisted a call to NJ.

   - A user dials 9 0 908 956 1234.
   - Communication Manager drops the ARS FAC (9 in our example), looks at the ARS Digit Analysis Table for 0, and analyzes the number. Then it:

     determines that more than 1 digit was dialed

     rules out the plan for 00, 01, and 011

     determines that 11 digits were dialed
   - Communication Manager routes the call to route pattern 1 as an operator assisted call.

Defining Inter-exchange carrier calls

About this task

Here is an example of how Communication Manager routes an ARS call to an inter-exchange (long-distance) carrier (IXC). IXC numbers directly access your long-distance carrier lines. IXC numbers begin with 1010, followed by three digits, plus the number as it is normally dialed including 0, 00, or 1+ 10 digits. These numbers are set up on your default translations. Remember, the user dials 9 to access ARS, then the rest of the number.

Procedure

1. Type `display ars analysis 1`.
2. Press **Enter** to view the ARS Digit Analysis Table screen starting with 1.

   This table shows five translations for IXC calls.

   When you use `x` in the **Dialed String** field, Communication Manager recognizes `x` as a wildcard. The `x` represents any digit, 0 - 9. If I dial 1010, the next 3 digits will always match the x wild cards in the dialed string.

Use the ARS digit analysis table shown above and follow the routing for an IXC call to AT&T. 1010288 is the carrier access code for AT&T.

- A user dials 9 1010288 plus a public network number.
- Communication Manager drops the ARS FAC (9 in our example), looks at the ARS Digit Analysis Table for 1010, and analyzes the number.
- Then it matches 288 with xxx and sends the call over route pattern 5.

Restricting area codes and prefixes

About this task

Certain area code numbers are set aside in the North American Numbering Plan. These numbers are 200, 300, 400, 500, 600, 700, 800, 877, 888, 900. You need to specifically deny calls made to area codes 200 through 900 (except 800 and 888).

You can also deny access to the 976 prefix, which is set aside in each area code for pay-per call services, if you do not want to incur charges. You can block 976 or any other prefix in all NPAs with a single entry in the digit analysis table. See *Using wild cards* for more information.

Procedure

1. Set the 200 area code apart from other area codes 201 through 209.

   We use the digit analysis table 120 because it defines long distance calls that begin with 1 and all area codes from 200 through 209.

2. To deny long distance calls to the 200 area code, type `change ars analysis 120`.
3. Press **Enter** to view the ARS Digit Analysis Table screen beginning with 120.

   The table (on the screen) in this example shows two translations for calls that begin with 120.

   First, follow the routing for a long-distance call that begins with 120 and is allowed. The 120 translation handles all dial strings 1-201 through 1-209, and there are many matches.

   - A user dials 9 120 plus 8 digits (the first of the 8 digits is not 0).
   - Communication Manager drops the ARS FAC (9 in our example), looks at the **ARS Digit Analysis Table** for 120, and analyzes the number. It determines the call is long-distance and sends the call over route pattern 4

   Now we will follow a call that begins with the restricted area code 200. Only one string matches this translation.

   - A user dials 9 1200 plus 7 digits.
   - Communication Manager drops the ARS FAC (9), and looks at the **ARS Digit Analysis Table** for 1200. It determines that the call type is deny, and the call does not go through.

Using wild cards

About this task

You can use wild cards to help separate out calls to certain numbers. Ensure that when you use the wild card `x` in the **Dialed String** field, Communication Manager recognizes `x` as any digit between 0 - 9. For example, you can restrict users from making calls to a 555 information operator where you might incur charges.

Procedure

1. Type `change ars analysis 1`.
2. Click **Enter**.

   The system displays the ARS Digit Analysis Table screen beginning with 1.
3. Use the arrow keys to move to a blank **Dialed String** field.
4. Type `1xxx555` in the **Dialed String** field.
5. Type `11` in the **Total Min** and `11` in **Total Max** fields.
6. Type `deny` (denied) in the **Route Pattern** field.
7. Type `fnhp` in the **Call Type** field.
8. Click **Enter** to save your changes.

Defining local information calls

About this task

You can set up Communication Manager to allow calls to local information, or in this example, 411.

To allow 411 service calls:

Procedure

1. Type `change ars analysis 4`.
2. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen beginning with 4.
3. Use the arrow keys to move to a blank **Dialed String** field.
4. Enter `411` in the **Dialed String** field.
5. Enter `3` in the **Total Min** and `3` in **Total Max** fields.
6. Enter `1` in the **Route Pattern** field.
7. Enter `svcl` (service call) in the **Call Type** field.
8. Press **Enter** to save your changes.

Administering Call Type Digit Analysis

Before you begin

There must be at least one entry in **Call Type Digit Analysis Table** to begin Call Type Digit Analysis.

Procedure

1. On the SAT command line interface, type `change call type analysis`.

   The system displays **Call Type Digit Analysis Table**.

2. In the **Match** field, type the digits the system uses to match with the dialed string.

   The dialed string contains the digits that Communication Manager analyzes to process the call.

   For example, type `303` to match the dialed numbers beginning with 303.

3. In the **length: Min Max** fields, type the minimum number and maximum number of dialed digits.

4. Type four digit manipulations for the **Match** string.

5. Type the number of digits for the system to delete or insert and select the call type. the system will delete, the number of digits the system will insert, and the call type against which the system will test the modified digit string.

Call Type Digit Analysis Example

In our example, this is the administered **Call Type Digit Analysis Table**.

In our example, Communication Manager analyzes 3035554927 for routing.

1. Communication Manager deletes 0 digits, inserts nothing, and searches the resulting 3035554927 against the ARS tables.
2. If there are no matching entries, Communication Manager deletes 0 digits, inserts the digit `1`, and searches the resulting 13035554927 against the ARS tables.
3. If there are no matching entries, Communication Manager deletes 3 digits, inserts nothing, and searches the resulting 5554927 against numbers of **ext** type in the dial plan.
4. If there are no matching entries, Communication Manager deletes 0 digits, inserts `011`, and searches the resulting 0113035554927 against the ARS tables.

Setting up Multiple Locations

Before you begin

Ensure that the **Multiple Locations** field on the System Parameters Customer-Options (Optional Features) screen is set to y. If this field is set to n, go to the Avaya Support website at http://support.avaya.com 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.

Multiple locations are supported only in the dedicated instance deployment. In case of multitenant deployment, each tenant is limited to one location.

Ensure your daylight saving rules are administered. Daylight Saving Rule numbers are located on the Daylight Saving Rules screen.

Each cabinet in a server or switch and each port network in the cabinet must be assigned a location number. See the `add-cabinet` and `change-cabinet` in *Maintenance Commands for Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

About this task

You can define a location number for:

- Remote Offices
- Gateways
- IP network regions, used by IP stations and IP trunks

You can create numbering plans and time zone and daylight saving plans that are specific for each location. Choose your main location, and offset the local time for each location relative to the system clock time. The main location is typically set to have offset 0.

For example, we will set up multiple locations for Communication Manager server with cabinets in Chicago and New York. Location 1 is assigned to the cabinet in Chicago, our main office, so Central Standard Time is used for our main location. Location 2 is assigned to the cabinet in New York. We'll define the numbering plan area (NPA) for the Chicago and New York locations, and set the time zone offset for NY to show the difference in time between Eastern Standard Time and Central Standard Time.

Tip:

Type `list cabinets` to see the Cabinet screen and a list of cabinets and their locations.

To define locations for cabinets in Chicago and New York:

Procedure

1. Type `change locations`.
2. Press `Enter`.

   The system displays the Locations screen.
3. Type `y` in the **ARS Prefix 1 required for 10-digit NANP calls** field.

   Our dial plan requires users to dial a `1` before all 10-digit (long distance) NANP calls.
4. Type `Chicago` in the **Name** field in the **Number 1 row**.

   Use this field to identify the location.
5. Type `+00:00` in the **TimeZone Offset** field in the **Number 1 row**.

   In our example, the system time and the Chicago location time are the same.

6. Type `1` in the **Daylight Saving Rule** field in the **Number 1 row**.

   In our example, daylight saving rule 1 applies to U.S. daylight saving time.

   Tip:

   Use the `display daylight-savings-rules` command to see what rules have been administered on Communication Manager.

7. Type `312` in the **Number Plan Area Code** field in the **Number 1 row**.

   In our example, 312 is the local area code for Chicago, location 1.

8. Type `New York` in the **Name** field in the **Number 2 row**

9. Type `-01:00` in the **TimeZone Offset** field in the **Number 2 row**.

   In our example, subtract one hour from the system clock in Chicago to provide the correct time for the location in New York.

10. Type `1` in the **Daylight Saving Rule** field in the **Number 2 row**.

    In our example, daylight saving rule 1 applies to U.S. daylight saving time, and both locations use the same rule.

11. Type `212` in the **NANP** field in the **Number 2 row**.

    In our example, 212 is the local area code for New York, location 2.

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

    See *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for more information on the Multiple Locations feature.

Routing with multiple locations

Before you begin

Be sure the **Multiple Locations** field on the System Parameters Customer-Options (Optional Features) screen is set to y. If this field is set to n, go to the Avaya Support website at http://support.avaya.com for more information.

To administer AAR and ARS, do the following:

- 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
- Gateways

- IP network regions, used by IP stations and IP trunks

For information on how to administer the location per station, see the Administer location per station on page 140 section.

For information on the description of the **Location** field on the Stations with Off-PBX Telephone Integration screen, see the *Avaya Aura® Communication Manager Screen Reference*.

About this task

When you set up multiple locations, you can define call routing that covers all locations as well as call routing specific to each individual location. Use your routing tables to define local routing for 911, service operators, local operator access, and all local calls for each location. Leave long-distance and international numbers that apply across all locations on the routing tables with **Location** field set to all.

For example, we will use ARS to set up local call routing for two Communication Manager server locations. Our Chicago server is assigned to location 1, and our New York server is assigned to location 2.

Our example shows a simple local dialing plan. Each location already contains location-specific routing tables. We'll use route pattern 1 for local service calls and route pattern 2 for local HNPA calls in the Chicago location.

Tip:

Create location-specific routing by assigning different route patterns for each location.

To define local calls for servers in Chicago and New York:

Procedure

1. Type `change ars analysis location 1`.
2. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen for location 1.
3. Type the information for local dialed strings and service calls in each row on the screen.

   In our example, for location 1 (Chicago) local HNPA calls:

   a. Type the appropriate digit in the **Dialed String** field.
   b. Type `7` in the **Total Min** field.
   c. Type `7` in the **Total Max** field.
   d. Type `2` in the **Route Pattern** field.
   e. Type `hnpa` in the **Call Type** field.

   In our example, for location 1 (Chicago) local service calls:

   a. Type the appropriate digits in the **Dialed String** field.
   b. Type `3` in the **Total Min** field.
   c. Type `3` in the **Total Max** field.
   d. Type `1` in the **Route Pattern** field.

e. Type `svcl` in the **Call Type** field.

4. Press **Enter** to save your changes.
5. Type `change ars analysis 4 location 2`.
6. Press **Enter**.

   The system displays the **ARS Digit Analysis Table** for location 2.
7. Type in the local HNPA and service call routing information for New York.
8. Press **Enter** to save your changes.

   See Automatic Routing in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for more information on ARS.

   See Multiple Locations in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205 for more information on the Multiple Locations feature.

Call routing modification

If your system uses ARS Digit Analysis to analyze dialed strings and select the best route for a call, you must change the digit analysis table to modify call routing. For example, you'll need to update this table to add new area codes or to restrict users from calling specific areas or countries.

Adding a new area code or prefix

Before you begin

A common task for system administrators is to configure their system to recognize new area codes or prefixes.

When you want to add a new area code or prefix, you look up the settings for the old area code or prefix and enter the same information for the new one.

Tip:

Use **display toll xxx**, where xxx is the prefix you want to add, to see if the new area code or prefix number is set up as a toll call (y) or not. Some users might be disallowed to dial toll call numbers.

About this task

We will add a new area code. When the California area code, 415, splits and portions change to 650, you will need to add this new area code to your system.

Tip:

If you do not need to use `1` for area code calls, omit the `1` in steps 1, 4, and 7 in our example. Also, enter `10` in the **Total Min** and **Total Max** fields (instead of 11) in step 8.

Procedure

1. Type `list ars route-chosen 14152223333`.
2. Press **Enter**.

   You can use any 7-digit number after 1 and the old area code (415). We used `222-3333`.

   The system displays the ARS Route Chosen Report screen.
3. Write down the **Total Min**, **Total Max**, **Route Pattern**, and **Call Type** values from this screen.

   In this example, the **Total Min** is **11**, **Total Max** is **11**, **Route Pattern** is **30**, and the **Call Type** is **fnpa**.
4. Type `change ars analysis 1650`.
5. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen.
6. Move to a blank **Dialed String** field.

   If the dialed string is already defined in your system, the system displays the cursor in the appropriate **Dialed String** field, where you can make changes.
7. Enter `1650` in the **Dialed String** field.
8. Enter the **minimum** and **maximum** values from step 2 in the **Total Mn** and **Total Mx** fields.

   In our example, enter `11` in each field.
9. Enter the `route pattern` from step 2 in the **Route Pattern** field.

   In our example, enter `30`
10. Enter `fnpa` in the **Call Type** field.
11. Enter the node number from step 2 in the **Node Num** field.

    For our example, leave the node number blank.
12. Press **ENTER** to save your changes.

    To add a new prefix, follow the same directions, except use a shorter dial string (such as list ars route-chosen 2223333, where 222 is the old prefix) and a dial type of `hnpa`.

    Tip:

    If you change an existing area code for a network with multiple locations, be sure to change the **Number Plan Area Code** field on the Locations screen.

Using ARS to restrict outgoing calls

About this task

With ARS, you can block outgoing calls to specific dialed strings. For example, you can restrict users from making international calls to countries where you do not do business, or in the U.S. you can restrict access to 900 and 976 pay-per-call numbers.

Security alert:

To prevent toll fraud, deny calls to countries where you do not do business. The following countries are currently concerns for fraudulent calling.

country	code	country	code
Colombia	57	Pakistan	92
Ivory Coast	225	Peru	51
Mali	23	Senegal	221
Nigeria	234	Yemen	967

To prevent callers from placing calls to Colombia (57):

Procedure

1. Type `change ars analysis 01157`.
2. Press **Enter**.
   a. Enter `011` (international access)
   b. Enter the `country code (57)`

   The system displays the ARS Digit Analysis Table screen.
3. Move to a blank **Dialed String** field.

   Skip to Step 6 to deny calls to this dialed string

   If the dialed string is already defined in your system, the system displays the cursor in the appropriate **Dialed String** field.
4. Enter `01157` in the **Dialed String** field.
5. Enter `10` in the **Total Min** and `23` in **Total Max** fields.
6. Enter `deny` (denied) in the **Route Pattern** field.
7. Enter `intl` in the **Call Type** field.
8. Press **Enter** to save your changes.

Overriding call restrictions

Before you begin

Verify that the **Authorization Codes** field on the System Parameters Customer-Options (Optional Features) screen is set to y.

Security alert:

You should make authorization codes as long as possible to increase the level of security. You can set the length of authorization codes on the Feature-Related System Parameters screen.

About this task

You can use authorization codes to enable callers to override a station's calling privileges. For example, you can give a supervisor an authorization code so they can make calls from a telephone that is usually restricted for these calls. Since each authorization code has its own COR, the system uses the COR assigned to the authorization code (and FRL assigned to the COR) to override the privileges associated with the employee's telephone.

Note that authorization codes do not override dialed strings that are denied. For example, if your ARS tables restrict users from placing calls to Colombia, a caller cannot override the restriction with an authorization code.

We will create an authorization code 4395721with a COR of 2.

Procedure

1. Type `change authorization-code 4395721`.
2. Press **Enter**.

   The system displays the Authorization Code - COR Mapping screen.
3. In the **AC** field, type `4395721`.
4. In the **COR** field, enter `2`.
5. Press **Enter** to save your changes.

ARS Partitions

Most companies want all their users to be able to make the same calls and follow the same route patterns. However, you might find it helpful to provide special calling permissions or restrictions to a group of users or to particular telephones.

With ARS partitioning, you can provide different call routing for a group of users or for specific telephones.

Note:

If you used partitioning on a prior release of Avaya Communication Manager and you want to continue to use partitioning, please read this section carefully. In this release of Avaya Communication Manager, partition groups are defined on the **Partition Route Table**. If you

want to define routing based on partition groups, use the **Partition Route Table**. Partition groups are no longer defined on the Digit Analysis Table.

Related links

Setting up Time of Day Routing on page 281

Setting up partition groups

Before you begin

- Ensure that the **Tenant Partitioning** field on the System Parameters Customer-Options (Optional Features) screen is `y`.
- Ensure that the **Time of Day Routing** field on the System Parameters Customer-Options (Optional Features) screen is `n`.

About this task

Let us say you allow your employees to make local, long distance, and emergency calls. However, you have a lobby telephone for visitors and you want to allow users to make only local, toll-free, and emergency calls from this telephone.

To restrict the lobby telephone, you modify the routing for a partition group to enable only specific calls, such as U.S. based toll-free 1-800 calls, and then assign this partition group to the lobby telephone.

To enable 1-800 calls for partition group 2:

Procedure

1. Type `list ars route-chosen 18002221000`.
2. Press **Enter**.

   You can use any 7-digit number following the 1800 to create an example of the dialed string.

   The system displays the ARS Route Chosen Report screen for `partition group 1`.
3. Record the route pattern for the selected dialed string.

   In our example, the route pattern for 1800 is p1. This indicates that the system uses the Partition Routing Table to determine which route pattern to use for each partition.

   Note:

   If there was a number (with no p) under Route Pattern on the Route Chosen Report, then all partitions use the same route pattern. You need to use the Partition Routing Table only if you want to use different route patterns for different partition groups.
4. Press **Cancel** to return to the command prompt.
5. Type `change partition-route-table index 1`.
6. Press **Enter**.

The system displays the Partition Routing Table screen. In our example, partition group 1 can make 1800 calls and these calls use route pattern 30.

7. In the **PGN2** column that corresponds to Route Index 1, type `30`.
8. Press **Enter**.

   This tells the system to use route pattern 30 for partition group 2 and allow partition group 2 members to make calls to 1800 numbers.

Assigning a telephone to a partition group

Before you begin

To assign an extension to a partition group, first assign the partition group to a COR, and then assign that COR to the extension.

Procedure

1. Type `list cor`.
2. Press **Enter**.
3. The system displays the Class of Restriction Information screen.
4. Choose a COR that has not been used.

   In our example, select 3
5. Type `change cor 3`.
6. Press **Enter**.

   The system displays the Class of Restriction screen.
7. Type a name for this COR in the **COR Description** field.

   In our example, type **lobby**
8. Enter `2` in the **Partitioned Group Number** field.
9. Now to assign `COR 3` to the lobby telephone at extension 1234:
   a. Type `change station 1234`.
   b. Press **Enter**.

      The system displays the Station screen for 1234.
   c. In the **COR** field, enter `3`.
   d. Press **Enter** to save your changes.

Setting up Time of Day Routing

Before you begin

AAR or ARS must be administered on Communication Manager before you use Time of Day Routing.

- For AAR, verify that either the **Private Networking** field or the **Uniform Dialing Plan** field is `y` on the System Parameters Customer-Options (Optional Features) screen.
- For ARS, verify that the **ARS** field is `y` and the **Time of Day Routing** field is `y` on the System Parameters Customer-Options (Optional Features) screen.

About this task

Time of Day Routing lets you redirect calls to coverage paths according to the time of day and day of the week. You need to define the coverage paths you want to use before you define the time of day coverage plan.

You can route calls based on the least expensive route according to the time of day and day of the week the call is made. You can also deny outgoing long-distance calls after business hours to help prevent toll fraud. Time of Day Routing applies to all AAR or ARS outgoing calls and trunks used for call forwarding to external numbers.

As an example, we will allow our executives to make long distance calls during business hours. Let us look at the Time of Day Routing Plan before we make any changes

To display your Time of Day Routing Plan:

Procedure

1. Type `display time-of-day 1`.
2. Press **Enter**.

   The system displays the Time Of Day Routing Plan screen for plan 1.

   Note:

   Make a note of the routing plan that is currently in effect. In our example, this plan is for employees who can only make local calls.

   You can see that in our example, two partition group numbers control time of day routing. PGN 1 begins one minute after midnight (00:01) every day of the week, and is used for after-business hours and all day Saturday and Sunday. PGN 2 is assigned to office hours Monday through Friday, not including noon (12:00) to 1:00 p.m. (13:00).
3. Press **Cancel** to clear the screen.

Creating a New Time of Day Routing Plan

Procedure

1. Type `change time-of-day 2`.
2. Press **Enter**.

3. Type `1` in each field as shown on **Time of Day Routing Plan 1**.

   In our example, this is the PGN used for after hours and the lunch hour.

4. Type `3` in all other fields.

   In our example, PGN 3 uses the route pattern for long-distance calls during business hours. We can save money by using the trunk lines provided by our new long-distance carrier.

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

6. Now assign your new Time of Day Routing Plan 2 to the COR assigned to your executives

   See *Class of Restriction* to view where to assign this field.

   For this example, assume the following:

   - Jim is the user at extension 1234.
   - Extension 1234 is assigned a COR of 2.
   - COR 2 is assigned a Time of Day Plan Number of 1.
   - The Time of Day Routing Plan 1 is administered as shown in the example above.

   When Jim comes into work on Monday morning at 8:30 and makes an ARS call (dials the ARS access code followed by the number of the person he is calling), the system checks the Time of Day Plan Number assigned to Jim's COR

   Because Jim has a COR of 2 with Time of Day Plan Number 1, the system uses Time of Day Routing Plan 1 to route the call.

   According to Time of Day Routing Plan 1, calls made between 8:00 a.m. and 11:59 a.m. route according to the route pattern set up on PGN 1.

   If Jim makes a call between 12:00 p.m. and 1:00 p.m. on Monday, the Time of Day Routing Plan 1 is used again. However, this time the call is routed according to PGN 2.

Setting up a Remote user by Network region and Time zone

About this task

With your system located in New York and a remote user located in Germany, to create the correct time zone settings:

Procedure

1. Type `change locations`.
2. Press `Enter`.

   The Locations screen displays.

3. In the **Name** field, enter the name of the location (for instance, Germany).
4. In the first **Timezone Offset** field, enter `+` to indicate the time is ahead of the system time.
5. In the second **Timezone Offset** field, enter `08` for the number of hours difference between this location and system time.
6. In the **Daylight Saving** field, enter `1` if this country has daylight saving.
7. Press `Enter` to save your changes.
8. Type `change ip-network-map`.
9. Press `Enter`.

   The IP Address Mapping screen displays.
10. In the **From IP Address** field, enter the IP address for the remote station in Germany.
11. In the **To IP Address** field, enter the IP address of your system.
12. In the **Subnet** or **Mask** field, enter the subnet mask value of your network
13. In the **Region** field, enter a number that is not being used. In this example, enter `3`.
14. Press `Enter` to save your changes.
15. Type `change ip-network-region 3`.
16. Press **Enter**.

    The IP Network Region screen displays.
17. In the **Name** field, enter the location name for familiarity.
18. In the **Location** field, enter the number from the Locations screen. In this example, it was `11`.
19. Press **Next Page** until you get to page 3, the Inter Network Region Connection Management screen.
20. Notice in the **src rgn** column that a 3 displays, and under **dst rgn** a 1, indicating that Network Region 3 (Germany) is connected to Network Region 1 (New York) using Codec Set 1.
21. Press `Enter` to save your changes

    See *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for more information on the Multiple Locations feature.

No-cadence call classification modes and End OCM timer

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

Setting up no-cadence call classification modes

About this task

Procedure

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

Setting up End OCM timer and announcement extension

About this task

Procedure

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

Alerting Tone for Outgoing Trunk Calls

Use the Alerting Tone for Outgoing Trunk Calls feature to apply an alerting tone to an outgoing trunk call after an administrable amount of time.

Setting the outgoing trunk alerting timer

Procedure

1. Enter change cor *n*, where *n* is the number of a specific COR.
2. Click **Next** until you see the **Outgoing Trunk Alerting Timer (minutes)** field.
3. In the **Outgoing Trunk Alerting Timer (minutes)** field, specify when the initial alerting tone must be applied to the call.
4. Select **Enter** to save your changes.

Setting the trunk alerting tone interval

Procedure

1. Enter change system-parameters features.

2. Click **Next** until you see the **Trunk Alerting Tone Interval (seconds)** field.
3. In the **Trunk Alerting Tone Interval (seconds)** field, specify the interval at which the alerting tone must be repeated on the call.
4. Select **Enter** to save your changes.

Chapter 12: Setting Up Telecommuting

Communication Manager Configuration for Telecommuting

Telecommuting emphasizes the ability to perform telephony activities while remote from Communication Manager. It is a combination of four features that permit you to remotely perform changes to your station's Coverage and Call Forwarding.

Note:

If you are operating in a Distributed Communications System (DCS) environment, you need to assign a different telecommuting-access extension to each Avaya server and tell your users which extension they should use. A user can set up call coverage from any of the DCS nodes, but needs to dial the telecommuting-access extension of the node on which their station is defined before using the feature access code. You can also set up telecommuting with an IP (internet protocol) telephone. See Adding an H.323 Softphone for more information.

- Coverage of Calls Redirected Off Net (Avaya IQON) allows you to redirect calls off your network onto the public network and bring back unanswered calls for further coverage.

  Note:

  If a call covers or forwards off-net and an answering machine answers the call, or it is directed to a cellular telephone and a cellular announcement is heard, the server views this call as an answered call. Communication Manager does not bring the call back to the server for further routing.

- You can use the Extended User Administration of Redirected Calls feature 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 Class of Restriction screen, see *Avaya Aura® Communication Manager Screen Reference*.
- 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. With the Personal Station Access feature, you can take your telephone, as long as the telephones are the same type, anywhere on the same server running Communication Manager.
- The Answer Supervision feature provides supervision of a call directed out of the server either by coverage or forwarding and determines whether Communication Manager should bring the call control back to its server.

Preparing to configure telecommuting

About this task

You can also set up telecommuting with an IP (internet protocol) telephone or IP Softphone. For example, see Adding an H.323 Softphone for more information.

Procedure

1. For DCP or ISDN telecommuting, ensure that you have the following equipment:
   - Call Classifier — Detector
   - 1264-TMx software
   - Communication Manager extender — switching module or standalone rack mount (Digital Communications Protocol (DCP) or Integrated Services Digital Network (ISDN))
   - For more information about this equipment, see the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.
2. Verify the following fields on the System Parameters Customer-Options (Optional Features) screen are set to **y**.

   For information about this screen, see *Avaya Aura® Communication Manager Screen Reference*.
   - **Cvg Of Calls Redirected Off-Net**
   - **Extended Cvg/Fwd Admin**
   - **Personal Station Access**
   - **Terminal Translation Initialization (TTI)**

   If neither Communication Manager extender nor the System Parameters Customer-Options (Optional Features) fields are configured, go to the Avaya Support website at http://support.avaya.com.
3. Verify the telecommuting access extension is a direct inward dialing (DID) or a central office (CO) trunk destination for off-premises features to work.
4. Configure **TTI** for personal station access (PSA).

   For information about configuring TTI, see Personal Station Access setup.
5. Configure Security Violation Notification for Station Security Codes.

   For information about Security Violation Notification, see Security Violations Notification setup.

Configuring telecommuting example

About this task

In our example, we set up the telecommuting extension and enable coverage of calls redirected off-net.

Procedure

1. Enter `change telecommuting-access`.
2. In the **Telecommuting Access Extension** field, enter `1234`.

   This is the extension you are configuring for telecommuting.
3. Enter `change system-parameters coverage`.
4. In the **Coverage Of Calls Redirected Off-Net Enabled** field, enter `y`.

   See Telecommuting Access in *Avaya Aura® Communication Manager Screen Reference*, for information about and field descriptions on the Telecommuting Access screen.

Personal Station Access setup

With Personal Station Access (PSA, you can 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.

Using the disassociate function within PSA, you can 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 unanswered. If the coverage point is a display telephone, the display shows `da` for “do not answer.” If the coverage point is a voice-messaging system, the messaging system receives an indication from Communication Manager that this call was unanswered, and treats the call accordingly.

Note:

Once a telephone has been associated with an extension, anyone using the terminal has the capabilities of the associated station. Be sure to execute a dissociate request if the terminal can be accessed by unauthorized users. This is particularly important if you use PSA and DCP extenders to permit remote DCP access.

Preparing to set up Personal Station Access

Procedure

1. Verify that the **Personal Station Access** field is set to `y` on the Class of Service screen.

   For information about this screen, see *Avaya Aura® Communication Manager Screen Reference*.

2. Verify that the extension has a COS that allows PSA.

Setting up Personal Station Access example

About this task

In our example, we specify the TTI State, the Record PSA/TTI Transactions, the class of service, and the feature access codes set up for PSA.

Procedure

1. Enter `change system-parameters features`.
2. Complete the following fields.
   a. Enter `voice` in the **TTI State** field.
   b. (Optional) Enter `y` in the **Log CTA/PSA/TTI Transactions in History Log** field.

      These fields display only when the **Terminal Translation Initialization (TTI) Enabled** field on this screen is set to `y`.
3. Enter `change cos`.
4. Enter `y` in the**Personal Station Access (PSA) 1** field.
5. Enter **`change feature-access-codes`**.
6. Complete the following fields.
   a. Enter `#4`in the **Personal Station Access (PSA) Associate Code** field.

      This is the feature access code you will use to activate Personal Station Access at a telephone.
   b. Enter `#3` in the **Dissociate Code** field.

      This is the feature access code you will use to deactivate Personal Station Access at a telephone.

   See Telecommuting settings changes for information on how to associate or disassociate PSA.

   See Enterprise Mobility User for information on how to set up the Enterprise Mobility User feature.

Related links

Telecommuting settings changes on page 299
Enterprise Mobility User on page 175

Placing calls from PSA-dissociated stations

About this task

You can allow users to place emergency and other calls from telephones that have been dissociated. To enable this:

Procedure

1. Assign a class of restriction (COR) for PSA-dissociated telephones.

   You do this on the Feature-Related System Parameters screen.

2. Set the restrictions for this COR on the Class of Restriction screen.

   If you want users to be able to place emergency calls from dissociated telephones, it is also a good idea to have the system send calling party number (CPN) or automatic number identification (ANI) information for these calls. To do this, you must set the **CPN, ANI for Dissociated Sets** field to `y` on the Feature-Related System Parameters screen.

Station Security Code setup

A Station Security Code (SSC) provides security to a station user by preventing other users from accessing functions associated with the user's station. Each station user can change their own SSC if they know the station's current settings.

You must create a system-wide SSC change feature access code (FAC) before users can change their SSC. You must also provide users with their individual SSC. A user cannot change a blank SSC.

Creating a Station Security Code example

About this task

In our example, we set the station security code for a user. For information about the screens referred in this topic, see *Avaya Aura® Communication Manager Screen Reference*.

Procedure

1. Enter `change feature-access-codes`.
2. Enter `#5` in the **Station Security Code Change Access Code** field.
3. Enter `change system-parameters security`.
4. Enter `4` in the `Minimum Station Security Code Length` field.

   This determines the minimum required length of the Station Security Codes you enter on the Station screen. Longer codes are more secure. If station security codes are used for external access to telecommuting features, the minimum length should be 7 or 8.

5. Enter `change station 1234`.

This is the station extension you configured for telecommuting.

6. Enter `4321` in the **Security Code** field.

   See *Avaya Aura® Communication Manager Screen Reference*, for information about and field descriptions on the Station screen.

   For description of the Station Security Codes feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Assigning an Extender Password example

About this task

You can assign an extender password to a user using Communication Manager. You can assign one password for each Communication Manager port.

Use the Remote Extender Personal Computer in the server room to perform this procedure.

In this example, we will set a system-generated random password for a user named John Doe.

Procedure

1. Double-click the **Security** icon.
2. Double-click **User Password for User 01**.
3. Select **Enable Password** to enable the password.
4. Click **random**.

   This means that the password is a system generated random number. The system displays a 10-digit number in the `Password` field. Take note of this number, your user will need it at home to access the server running Communication Manager.
5. Enter `Doe, John` and click **OK**.

   This is the last name and first name of the user. The system returns you to the Password Manager screen.
6. Select **CommLink:Select Cards**.

   The system displays a screen containing a list of cards (for example, Card A, Card B, and so on). Each card corresponds to a port on your Avaya Server.
7. Select **Card A** and click **OK**.
8. Select **CommLink:Upload Password**.

   The system displays the error message screen with the message "`Administrator password not loaded`".
9. Click **OK**.
10. Enter `123456` and click **OK**.

11. Select **CommLink:Upload Password**.
12. When upload is complete, click `OK`.
13. Select **File:Save As**.
14. Enter `doe.fil` in the **File** field and click **OK** to save your changes.

Call Forwarding setup for telecommuting

You can change your call forwarding from any on-site or off-site location using Communication Manager.

Setting up Call Forwarding for telecommuting example

About this task

In our example, we assign the feature access codes and class of service to set up call forwarding. Using which your users can forward their calls to another extension. For information about the screens referred in this topic, see *Avaya Aura® Communication Manager Screen Reference*.

Procedure

1. Enter `change feature-access-codes`.
2. Set a 2-digit access code for the following fields.
   a. Enter `Extended Call Fwd Activate Busy D/A` field.
   b. Enter `*7` in the **Extended Call Fwd Activate All** field.
   c. Enter `*6` in the **Extended Call Fwd Activate Deactivation** field.

   This sets the access codes for these features. The system displays the Command prompt.
3. Enter `change cos`.
4. Set the following fields to`y`.
   - **Extended Forwarding All**
   - **Extended Forwarding B/DA**

   You can change the forwarding of all your calls from an off-site location using this.
5. Set the **Restrict Call Fwd-Off Net** field to `n`.

   See *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205*,* for a description of the Call Forwarding feature.

   See *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for a description of the Tenant Partitioning feature.

   See Telecommuting settings changes for information on how to change call forwarding.

Interactions for Call Forwarding

- Bridged Appearance

  When the pound key (#) is pressed from a bridged appearance immediately following any of this feature's four feature access codes (FACs), the system assumes that the currently active bridged extension will be administered. The station security code of the currently active bridged extension must be entered after the initial # to successfully complete the command sequence.

  If the station has only bridged appearances, the station's extension must be dialed after the FAC to successfully complete the command sequence, since the station's extension is not associated with any appearances.

- Distributed Communications System

  Assign a different telecommuting access extension for each server running Communication Manager. You can use Extended User Administration of Redirected Calls from any of the DCS nodes, but you must dial the extension of the node on which your station is defined before dialing the FAC.

- Tenant Partitioning

  The telecommuting access extension is always automatically assigned to Tenant Partition 1, so it can be accessed by all tenants.

  The tenant number of the extension being administered must be accessible by the tenant number from which the Extended User Administration of Redirected Calls FAC is dialed or the request is denied. If the FAC is dialed on site, the tenant number of the station or attendant must have access to the tenant number of the extension administered. If the FAC is dialed off site, the tenant number of the incoming trunk must have access to the tenant number of the extension administered.

Coverage options assignment for telecommuting

You can use Communication Manager to assign two previously administered coverage paths and/or time of day coverage tables on the Station screen. Using which telecommuters can alternate between the two coverage paths and/or time of day coverage tables administered to control how their telephone calls are handled.

For information about creating a coverage path, see Creating coverage paths.

For information about creating a time of day coverage table, see Assigning a coverage path to users.

See Telecommuting settings changes for information on how to alternate your coverage path option.

Related links

Assigning a coverage path to users on page 206

Creating coverage paths on page 205
Telecommuting settings changes on page 299

Assigning coverage for telecommuting example

About this task

In our example, we assign two coverage options so a user can choose from either option to control how their calls are handled. For information about the screens referred in this topic, see *Avaya Aura® Communication Manager Screen Reference*.

Procedure

1. Enter `change feature-access-codes`.
2. Enter `#9` in the **Change Coverage Access Code** field.
3. Enter `change cor 1`.
4. In the **Can Change Coverage** field, enter `y` and select `Enter` to save your changes.
5. Enter `change station 1234`.

   This is the station extension you configured for telecommuting. The system displays the Station screen.
6. Complete the following fields:
   a. Enter `2` in the **Coverage Path 1** field.
   b. Enter `8` in the **Coverage Path 2** field.

   See Coverage Path in *Avaya Aura® Communication Manager Screen Reference*, for information about and field descriptions on the Coverage Path screen.

   See *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for a description of the Call Coverage feature.

   See *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for information about the Extended User Administration of Redirected Calls feature.

Home Equipment Installation

You can use Communication Manager to install equipment in your home so that you can use system facilities from off-site.

See Communication Manager Configuration for Telecommuting for step-by-step instructions on how to configure your office equipment.

See Telecommuting settings changes for step-by-step instructions on how to use your home station.

Preparing to install home equipment

About this task

You can also set up telecommuting with an IP (internet protocol) telephone or IP Softphone. For example, see Adding an H.323 Softphone for more information.

Procedure

1. For DCP telecommuting, verify that you have the following equipment:
   - Communication Manager extender remote module
   - DCP sets (office and home must match)
2. Configure a feature access code for associating your home number to your office number.

   For information about configuring an associate feature access code, see Personal Station Access setup.

Installing home equipment example

Procedure

1. Plug the telephone cord into the slot labeled line on the back of the module and into the wall jack.
2. Plug the telephone cord into the slot labeled port on the back of the module and into the slot labeled line on the telephone.
3. Plug the power cord into slot labeled turn on the back of the module and the wall socket.

   The system displays `Go Online` on the telephone display.
4. Press `3 (Nxt)`.

   The system displays `Set Phone Number` on the telephone display.
5. Press `2 (OK)` to set the telephone number.
6. Enter `5551234` and press `Drop`.

   This is the assigned analog telephone number. In some areas, you might need to include your area code (for example, 3035551234). The system displays `Set Phone Number` on the telephone display.
7. Press `1(Prv)`.

   This returns you to the `Go Online` telephone display.
8. Press `2 (OK)`.

   The module dials the number. When the modules connect, the telephone displays `Enter Password`.
9. Enter `0123456789` and press `Drop`.

Associating your office telephone number to the home station example

Procedure

1. On your home station, enter `#4`.

   This is the associate feature access code.

2. Enter `4321` and press `#`.

   This is your extension number.

3. Enter `1996` press `#`.

   This is your password.

Disassociating your home station

Procedure

Press `Hold` four times.

Remote Access setup

Remote Access provides you with access to the system and its features from the public network. Using which you can make business calls from home or use Recorded Telephone Dictation Access to dictate a letter. If authorized, you can also access system features from any on-site extension.

With Remote Access you can dial into the system using Direct Inward Dialing (DID), Central Office (CO), Foreign Exchange (FX), or 800 Service trunks. When a call comes in on a trunk group dedicated to Remote Access, the system routes the call to the Remote Access extension you have assigned. If DID is provided and the Remote Access extension is within the range of numbers that can be accessed by DID, Remote Access is accessed through DID.

Barrier codes provide your system security and define calling privileges through the administered COR. You can administer up to 10 barrier codes, each with a different COR and COS. Barrier codes can be from 4 to 7 digits, *but all codes must be the same length*. You can also require that users enter an authorization code to use this feature. Both barrier codes and authorization codes are described under Authorization Codes setup.

See *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for a description of the Remote Access feature.

Security alert:

Avaya has designed the Remote Access feature incorporated in this product that, when properly administered by the customer, will enable the customer to minimize the ability of unauthorized persons to gain access to the network. It is the customer’s responsibility to take the appropriate steps to properly implement the features, evaluate and administer the various restriction levels, protect access codes and distribute them only to individuals who have been

advised of the sensitive nature of the access information. Each authorized user should be instructed concerning the proper use and handling of access codes.

In rare instances, unauthorized individuals make connections to the telecommunications network through use of remote access features. In such an event, applicable tariffs require that the customer pay all network charges for traffic. Avaya cannot be responsible for such charges, and will not make any allowance or give any credit for charges that result from unauthorized access.

If you do not intend to use Remote Access now or in the future, you can permanently disable the feature. If you do decide to permanently disable the feature, it will require Avaya Services intervention to activate the feature again.

Preparing to setup Remote Access

Procedure

1. Configure the **Incoming Destination** and **Night Service** fields on the CO Trunk screen.

   For information about configuring a CO trunk, see CO, FX, or WATS trunk group administration.

2. Verify that the **Authorization Codes** field on the System Parameters Customer-Options (Optional Features) screen is set to y.
3. Verify that the **SVN Authorization Code Violation Notification Enabled** field on the Security-Related System Parameters screen is set to y.

Setting up remote access example

About this task

In our example, we set up a remote access extension with maximum security. This assists you in blocking unauthorized people from gaining access to your network.

Procedure

1. Enter `change remote-access` and select `Enter`.
2. On the Remote Access screen enter `1234` in the **Remote Access Extension** field.

   This is the extension specified in the **Incoming Destination** field on the CO Trunk screen.

3. Enter `7` in the **Barrier Code Length** field.

   This is the number of digits your barrier code must be when entered.

4. Enter `y` in the **Authorization Code Required** field.

   This means you must also enter an authorization code when you access the system's Remote Access facilities. For information about setting up access codes, see Authorization Codes setup.

5. Enter`y` in the **Remote Access Dial Tone** field.

This means you hear dial tone as a prompt to enter your authorization code.

6. Enter `1234567` in the **Barrier Code** field.

   This is the 7-digit barrier code you must enter to access the system's Remote Access facilities.

7. Type `1` in the **COR** field.

   This is the class of restriction (COR) number associated with the barrier code that defines the call restriction features.

8. Enter `1` in the `TN` field.

   This is the Tenant Partition (TN) number.

9. Enter `1` in the **COS** field.

   This is the class of service (COS) number associated with the barrier code that defines access permissions for Call Processing features.

10. Type the expiration date in the **Expiration Date** field.

    This is the date the barrier code expires. A warning message is displayed on the system copyright screen seven days before the expiration date. The system administrator can modify the expiration date to extend the time interval, if necessary.

11. Enter `y` in the **Disable Following A Security Violation** field.

    This disables the remote access feature following detection of a remote access security violation.

12. Select `Enter` to save your work.

Disabling remote access permanently

Procedure

1. Enter `change remote-access`.
2. Enter `y` in the **Permanently Disable** field.

   If you permanently disable this feature, it requires Avaya Services intervention to reactivate the feature. There is a charge for reactivation of this feature.

3. Select `Enter` to save your work.

   Caution:

   Your attempt to disable the Remote Access feature will be lost if the server running Communication Manager is rebooted without saving translations. Therefore, execute a **`save translation`** command after permanently disabling the Remote Access feature.

Secure Shell remote login

Using Secure Shell (SSH), you can log in remotely to the following:

- Supported gateways
- Supported servers
- Communication Manager SAT interface on an Avaya common server using port 5022.

The SSH capability provides a secure method for remote access. For more information on supported servers and gateways, see *Avaya Aura® Communication Manager Hardware Description and Reference* guide.

Note:

You must set up the client device for remote login and configure the device for SSH. For information about understanding the relevant commands for SSH, see your client PC documentation.

Telecommuting settings changes

You can use Communication Manager to associate and disassociate PSA, change the coverage path for your station, change the extension to which you forward your calls, and change your personal station's security code.

Changing Telecommuting settings

Procedure

1. Configure PSA.

   For information about configuring PSA, see Personal Station Access setup.

2. Assign two coverage options for your system.

   For information on how to assign coverage options, see Coverage options assignment for telecommuting.

3. Configure call forwarding for your system.

   For information about configuring call forwarding, see Call Forwarding setup for telecommuting.

4. Configure security codes for a station.

   For information about configuring personal station security codes, see Assigning an Extender Password example.

Associating PSA example

About this task

In this example, we associate PSA (preferences and permissions) assigned to your station with another compatible terminal.

Procedure

1. Dial **#4**.

   This is the associate PSA feature access code. You hear dial tone.

2. Enter **1234** and press #.

   This is your extension.

3. Enter **4321** and press #.

   This is your Station Security Code. You hear a confirmation tone.

Disassociating PSA example

About this task

In our example, we disassociate PSA from the station you are using.

Procedure

Dial #3.

This is the disassociate PSA feature access code. You are no longer PSA associated to this station.

Changing a coverage option example

About this task

In this example, we change the coverage option from path 1 to path 2 from a remote location.

Procedure

1. Dial 1234.

   This is the extension you configured for telecommuting. You hear dial tone.

2. Dial #9 and press #.

   This is the feature access code you set for changing a coverage path. You hear dial tone.

3. Dial 4321 and press #.

   This is the extension for which you want to change the coverage path.

4. Dial 87654321.

   Press #.

This is the extension security code.

5. Dial `2`.

   This is the new coverage path. You hear confirmation tone.

Changing call forwarding example

About this task

In this example, we change call forwarding to extension 1235.

Procedure

1. Dial `1234`.

   This is the extension you configured for telecommuting.

2. Dial **#8** and press `#`.

   This is the feature access code you set for activating extended call forward. You hear dial tone.

3. Dial `4321` and press `#`.

   This is the extension from which you want to forward calls.

4. Dial `87654321` and press `#`.

   This is the extension security code. You hear dial tone.

5. Dial `1235`.

   This is the extension to which you want to forward calls. You hear the confirmation tone.

Changing your personal station security codes example

About this task

In this example, we change the security code for extension 1235 from 98765432 to 12345678.

Procedure

1. Dial `#5`.

   This is the feature access code you set for changing your security code. You hear dial tone.

2. Dial `1235` and press `#`.

   This is the extension for which you want to change the security code.

3. Dial `98765432` and press `#`.

   This is the current security code for the extension. You hear dial tone.

4. Dial `12345678` and press `#`.

   This is the new security code. Security codes can be 3-8 digits long.

5. Dial `12345678`.

   Press **#**.

   This is to confirm your new security code. You hear the confirmation tone.

   Note:

   If you cannot change your security code, Manager 1 can clear the problem using the **`Clear Audit Summary`** command.

Interrupting the command sequence for personal station security codes

Procedure

1. To interrupt the command sequence before step 3, choose one of these options:
   - Disconnect or press the disconnect or recall button before hearing intercept tone in step 3.

     The system does not log an invalid attempt. You must restart the process at step 1.
   - Type * before the second # in step 3.

     You must begin the change sequence at the point of entering your extension in step 2. (You should not enter the FAC again.)
   - Type * after the FAC has been entered and before the final #.

     You must restart the process at step 1.
2. To interrupt the command sequence after step 3, type * in steps 4 or 5, you must begin the change sequence at the point of entering the new station security code (SSC) in step 4.

   If you hear intercept tone in any step, the command sequence has been invalidated for some reason and you must restart the process at step 1.

   If you hear intercept tone after step 3, the system logs an invalid attempt via the Security Violations Notification (SVN) feature. This is true even if you attempt to interrupt the change sequence with an asterisk.

Chapter 13: Enhancing System Security

Basic Security recommendations

System security

You can refer to the following checklist to keep your system secure.

No.	Task	Description	Notes	✔
1.	Use Enhanced Access Security Gateway to log in to Communication Manager, and secure both system administration and maintenance ports. Customers with maintenance contracts have access to the optional password authentication interface program.	-		
2.	While attempting to gain access to the system, activate Security Violations Notification (SVN) to report unsuccessful attempts. Following a security violation, SVN automatically disables: • A valid login ID • Remote access for a barrier code or an authorization code	-		

Table continues…

No.	Task	Description	Notes	✔
3.	Use the following to secure trunks: • Automatic Route Selection (ARS) • Class of Restriction (COR) • Facility Restriction Levels (FRL) • Alternate Facility Restriction Levels (AFRLs) • Authorization Codes • Automatic Circuit Assurance (ACA) • Forced Entry of Account Codes	For more information about Call Detail Recording, see *Avaya Aura® Communication Manager Feature Description and Implementation, 555-245-205*.		
4.	For remote access, use Secure Shell (SSH) as a secure protocol. The SSH capability provides a high level of security during remote access. A system administrator uses the SSH capability to disable Telnet when Telnet is not required.	-		
5.	Activate Enhanced Call Transfer for your voice messaging system, if available. This call facility limits transfers to valid extensions. But you must restrict transfers to extensions that can offer dial tone to the caller, such as screen extensions.	-		

System security

You can refer to the following checklist to keep your system secure. For more information about the various features related to security, see the *Avaya Toll Fraud and Security Handbook*, 555-025-600 Guide.

1. Use Enhanced Access Security Gateway to log in to Communication Manager, and secure both system administration and maintenance ports. Customers with maintenance contracts have access to the optional password authentication interface program.
2. Activate Security Violations Notification (SVN) to report unsuccessful attempts to access the system. Security Violations Notification lets you automatically disable a valid login ID following a security violation involving that login ID and disable remote access following a security violation involving a barrier code or authorization code.
3. Secure trunks using Automatic Route Selection (ARS), Class of Restriction (COR), Facility Restriction Levels (FRLs) and Alternate Facility Restriction Levels (AFRLs), Authorization Codes, Automatic Circuit Assurance (ACA), and Forced Entry of Account Codes (see Call Detail Recording in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for more information).

4. You can log in remotely using Secure Shell (SSH) as a secure protocol. The SSH capability provides a highly secure method for remote access. A system administrator can use the capability to disable Telnet when it is not needed, making for a more secure system.
5. Activate Enhanced Call Transfer for your voice messaging system, if available. This limits transfers to valid extensions, but you must restrict transfers to extensions that can offer dial tone to the caller, such as screen extensions.

Toll Fraud prevention

Preventing toll fraud

Procedure

1. Protect system administration access.

   Make sure secure passwords exist for all logins using which System Administration or Maintenance can access 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 dialup maintenance port.

    Change the access password regularly and issue it only to authorized personnel. Consider activating Enhanced Access Security Gateway. For more information, see “Enhanced Access Security Gateway” in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

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, using which the unauthorized caller can 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 Personal Computer 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 or sell operations are conducted at public pay telephones located in subways, shopping malls, or airport locations. See Security Violations Notification setup to prevent this happening to your company.

Security Enforcement

To include an added layer of security, the user must implement the following safeguards to ensure physical security for Communication Manager:

- Unplug and secure attendant console handsets when the attendant position is not in use.
- Lock wiring closets and server rooms.
- Keep a log book register of technicians and visitors.
- Shred information about Communication Manager from folders that you discarded.
- Always demand verification of every technician or visitor by asking for a valid identification proof.
- Keep any reports related to trunk access codes, screen barrier codes, authorization codes, or password information secure.
- Keep the attendant console and supporting documentation in the office secured with a changeable combination lock.

  Provide the changeable combination number to people who need to enter the office.
- Keep any documentation related to the Communication Manager operation secure.
- Label all backup tapes or flash cards with correct dates to avoid using an outdated tape or flash card while restoring data.

  You must ensure that all backup media have the correct generic software load.

Checking system security

About this task

Here's some of the steps required for indemnification. Use these to analyze your system security.

Procedure

1. Remove all default factory logins of **cust**, **rcust**, **browse**, **nms**, and **bcms** and assign unique logins with 7-character alphanumeric passwords and a 90-day password aging.

   Use the **`list logins`** command to find out what logins are there.

2. If you do not use Remote Access, be sure to disable it permanently.

   Tip:

   You can use the **`display remote-access`** command to check the status of your remote access.

   To disable Remote Access, on the Remote Access screen, in the **Permanently Disable** field, enter `y`.

   Note:

   Avaya recommends that you permanently disable Remote Access using the **`change remote-access`** command. If you do permanently disable Remote Access, the code is removed from the software. Avaya charges a fee to restore the Remote Access feature.

3. If you use Remote Access, but only for internal calls, change announcements or remote service observing.
   a. Use a 7-digit barrier code.
   b. Assign a unique COR to the 7-digit barrier code.

      The unique COR must be administered where the **FRL** is `0`, the **Calling Party Restriction** field is `outward`, and the **Calling Permissions** field is `n` on all unique Trunk Group COR.

   c. Assign **Security Violation Notification Remote** to `10` attempts in `2` minutes.
   d. Set the aging cycle to `90` days with `100` call limit per barrier code.

4. If you use Remote Access to process calls off-net or in any way access the public network:
   a. Use a 7-digit barrier code.
   b. Assign a unique COR to the barrier code.
   c. Restrict the COR assigned to each barrier code by FRL level to only the required calling areas to conduct business.
   d. Set the aging cycle to `90` days with `100` call limit per barrier code.
   e. Suppress dial tone where applicable.

f. Administer Authorization Codes.

g. Use a minimum of 11 digits (combination of barrier codes and authorization codes).

h. Assign **Security Violation Notification Remote** to 10 attempts in 2 minutes.

5. If you use vectors:

   a. Assign all Vector Directory Numbers (VDN) a unique COR.

      See *Avaya Aura® Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568, and *Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780, for more information.

      Note:

      The COR associated with the VDN dictates the calling privileges of the VDN/vector. High susceptibility to toll fraud exists on vectors that have “collect digits” steps. When a vector collects digits, it processes those digits back to Communication Manager and if the COR of the VDN allows it to complete the call off-net, it will do so. For example, the announcement “If you know your party’s 4-digit extension number, enter it now” results in 4 digits being collected in step 6. If you input “90##” or “900#”, the 4 digits are analyzed and if “9” points towards ARS and “0” or “00” is assigned in the ARS Analysis Tables and the VDN COR allows it, the call routes out of the server to an outside local exchange or long distance operator. The operator then connects the call to the requested number.

   b. If vectors associated with the VDN do not require routing the call off-net or via AAR, assign a unique COR where the **FRL** is `0`, the **Calling Party Restriction** field is `outward`, the **Calling Permissions** field is `n` on all unique Trunk Group COR.

   c. If the vector has a “route-to” step that routes the call to a remote server via AAR, assign a unique COR with a unique ARS/AAR Partition Group, the lowest FRL to complete an AAR call, and `n` on all unique COR assigned to your public network trunking facilities on the Calling Permissions.

      Assign the appropriate AAR route patterns on the AAR Partition Group using the **`change aar analysis partition x 2`** command.

      Tip:

      You can use the **`display aar analysis print`** command to print a copy of your Automatic Alternate Routing (AAR) setup before making any changes. You can use the printout to correct any mistakes.

   d. If the vector has a “route-to” step that routes the call to off-net, assign a unique COR with a unique ARS/AAR Partition Group, the lowest FRL to complete an ARS call, and `n` on all unique COR assigned to your public network trunking facilities on the Calling Permissions.

      Assign the appropriate complete dial string in the “route-to” step of the vector the unique ARS Partition Group using the **`change ars analysis partition x 2`** command.

6. On the Feature Access Code (FAC) screen, **Facility Test Calls Access Code**, the **Data Origination Access Code**, and the **Data Privacy Access Code** fields, change from the default or remove them.

   For information about the Feature Access Code (FAC) screen, see *Avaya Aura® Communication Manager Screen Reference*.

   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*, 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*, for more information on Class of Service.

   Note:

   If a station is call forwarded off-net and an incoming call to the extension establishes using a loop-start trunk, incorrect disconnect supervision can occur at the Local Exchange Central Office when the call terminates. This gives the caller recall or transfer dial tone to establish a fraudulent call.

9. Administer Call Detail Recording on all trunk groups to record both incoming and outgoing calls.

   See Call information collection for more information.

10. On the Route Pattern screen, be careful assigning route patterns with an **FRL** of `0`; these allow access to outgoing trunking facilities.

    Avaya recommends assigning routes with an **FRL** of `1` or higher.

    Note:

    An exception might be assigning a route pattern with an **FRL** of `0` to be used for 911 calls so even restricted users can dial this in emergencies.

Tip:

You can use the **`list route-pattern print`** command to print a copy of your FRLs and check their status.

11. On all Trunk Group screens, set the **Dial Access** field to `n`.

    If set to `y`, users can dial Trunk Access Codes, thus bypassing all the ARS call screening functions.

    See the Trunk Group section of *Avaya Aura® Communication Manager Screen Reference*, 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*.

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*, 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. 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*, 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, 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.

16. 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*, for more information.
17. 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*, for more information.
18. Call Accounting Systems produce reports of call records.

    It detects telephones that are being hacked by recording the extension number, date and time of the call, and what digits were dialed.

User profile and login administration

Using the Authentication, Authorization, and Accounting (AAA) services, you can store and maintain administrator account or login information on a central server. Login authentication and access authorization are administered on the central server.

For more information about administering user profile and login, see *Avaya Aura® Communication Manager Feature Description and Implementation* and *Maintenance Commands for Avaya Aura® Communication Manager*.

Enhanced Access Security Gateway

For more information on Enhanced Access Security Gateway, see “Enhanced Access Security Gateway” in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

For more information on SVN, see “Security Violations Notification” in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Busy Verify for toll fraud detection

This section describes how to use the Busy Verify or Busy Verification feature to detect toll fraud.

If you suspect toll fraud, you can interrupt the call on a specified trunk group or an extension number and monitor the call in progress. Callers hear a tone during the call that indicates that the call is being monitored.

Security alert:

Listening to the call of another caller can be subject to federal, state, or local regulations. You might need the consent of one or both the parties on the call. Find out and comply with the applicable laws, rules, and regulations when you use the Busy Verify feature.

Preparing to use busy verify for toll fraud detection

Procedure

On the Trunk Group screen - page 1, verify the **Dial Access** field is `y`.

If it is not, go to the Avaya Support website at http://support.avaya.com.

Sample scenario to use the Busy Verify feature for toll fraud detection

Procedure

1. Type `change station` **xxxx**. The `busy verify` button is assigned to the **xxxx** station.
2. Press **Enter**.

   The system displays the Station screen. For this example, type extension `1014`.
3. Click **Next Page** until you see the **Site Data** fields.
4. In the **BUTTON ASSIGNMENTS** area, type `verify,` and press **Enter** to save your changes.
5. To activate the feature on the telephone, click the `Verify` button. Then type the `Trunk Access Code` and the member number to be monitored.

Authorization codes setup

Authorization codes extend call-privilege control to system users and provide an extra level of security for callers using remote access.

To maintain system security, Avaya recommends you to use authorization codes.

For more information about authorization codes setup, see *Avaya Toll Fraud and Security Handbook*, 555-025-600.

Preparing to setup Authorization Codes

Procedure

On the screen, verify the **Authorization Codes** field is `y`.

If not, go to the Avaya Support website at http://support.avaya.com. This field turns on the feature and permits you to selectively specify levels of calling privileges that override in-place restrictions.

Setting Up Authorization Codes example

Procedure

1. Enter **`change system-parameters features`** and press `Enter`.
2. Click **Next** until you find the **Authorization Code Enabled** field.
3. In the **Authorization Code Enabled** field, enter`y`.

   This enables the Authorization Codes feature on a system-wide basis.
4. In the **Authorization Code Length** field, enter `7`.

   This defines the length of the Authorization Codes your users need to enter. To maximize the security of your system, Avaya recommends you make each authorization code the maximum length allowed by the system.
5. In the **Authorization Code Cancellation Symbol** field, leave the default of `#`.

   This is the symbol a caller must dial to cancel the 10-second wait period during which your user can enter an authorization code.
6. In the **Attendant Time Out Flag** field, leave the default of `n`.

   This means a call is not to be routed to the attendant if a caller does not dial an authorization code within 10 seconds or dials an invalid authorization code.
7. In the **Display Authorization Code** field, enter `n`.

   This prevents the authorization code from displaying on telephone sets thus maximizing your security.
8. Select `Enter` to save your changes.
9. Enter `change authorization-code` **`nnnn`**, where **`nnnn`** is the authorization code, and press `Enter`.
10. In the **AC** field, enter the authorization code your users must dial.

    In this example, type `4285193`. The number of digits entered must agree with the number assigned in the Feature-Related System Parameters screen, **Authorization Code Length** field.

    Note:

    Remember, all authorization codes used in the system must be the same length.

11. In the **COR** field, enter the required Class of Restriction number from 0 through 95.

    In our example, type `1`.

12. Enter `change trunk-group` **`n`**, where **`n`** is the assigned trunk group number, and press `Enter`.

13. In the **Auth Code** field, enter `y` to require callers to enter an authorization code to tandem a call through an AAR or ARS route pattern.

    The code will be required even if the facility restriction level of the incoming trunk group is normally sufficient to send the call out over the route pattern.

14. Select `Enter` to save your changes.

Related information for Authorization Codes

See Class of Restriction in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for more information on setting up dialing out restrictions.

See *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504, for more information on using trunk access codes.

See Facility Restriction Levels and Traveling Class Marks *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205 and Route Pattern in *Avaya Aura® Communication Manager Screen Reference*, 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*, 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*, 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, Branch Gateways and Servers* for details on administering user profiles and logins.

Security Violations Notification setup

This section describes how to use Security Violations Notification (SVN) to set parameters related to security and to receive notifications when established limits exceed. You can run reports related to attempts of invalid access. 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 unsuccessful in the future. For more information about how to use SVN, see the *Avaya Toll Fraud and Security Handbook*, 555-025-600 Guide.

Sample scenario for setting up SVN

Procedure

1. Type `change system-parameters security`, and press `Enter` to open the Security-Related System Parameters screen.
2. Enter `y` in the **SVN Login Violation Notification Enabled** field.

   This sets Security Violations Notification login violation notification.

   Note:

   If you are not using Security Violation Notification for logins, enter`n` in the **SVN Login Violation Notification Enabled** field and go to Step 6.
3. In the **Originating Extension** field, enter `3040`.

   This becomes the telephone extension for the purpose of originating and identifying SVN referral calls for login security violations.
4. In the **Referral Destination** field, enter `attd` to send all calls to the attendant.

   This is the telephone extension that receives the referral call when a security violation occurs.
5. Select `Enter` to save your changes.

   Note:

   If you are not using Remote Access, go to Step 9.
6. (Optional) Type **`change remote-access`** and press `Enter`.
7. (Optional) In the **Disable Following A Security Violation** field, type `y`.

   This disables Remote Access following detection of a remote access security violation.
8. (Optional) Press `Enter` to save your changes.
9. Type **`change station xxxx`**, where **`xxxx`** is the station to be assigned the notification halt button and press `Enter`.
10. In the BUTTON ASSIGNMENTS section, type one of the following:
    - **`asvn-halt`** — The Authorization Code Security Violation Notification call is activated when an authorization code security violation is detected. This applies only if you are using authorization codes.
    - **`lsvn-halt`** — The Login Security Violation Notification call is activated a referral call when a login security violation is detected.

- **rsvn-halt** — The Remote Access Barrier Code Security Violation Notification call is activated as a call referral. This applies only if you are using Remote Access barrier codes.
- **ssvn-halt** — The Station Code Security Violation Notification call is activated when a station code security violation is detected. This applies only if you are using station codes.

Note:

Any of the above 4 security violations will cause the system to place a notification call to the designated telephone. The call continues to ring until answered. To stop notification of any further violations, press the button associated with the type of violation.

11. Press `Enter` to save your changes.

Enhanced security logging

Enhanced security logging increases the granularity of logging of user activity, using which you can specify an external server or Linux syslog to which Communication Manager can 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 server.

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 screen to enable or disable the ability to send logs to an external server, and to specify the logs to be sent.

Configuring syslog server

About this task

Use the Server Log Files page to select the logs that you want to send to an external syslog server. You can specify the types of logs that you want to send to remote servers. For example, Security, CM IP, Command, Kernel, and Messages.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, under **Security**, click **Server Log Files** and do the following:

4. In **Enabled**, select Yes or No.
5. In **Protocol**, click the method to transfer the syslogs.

   The options are:

   - **UDP**
   - **TCP**
   - **TLS**
6. In **Port**, type the port number of the remote syslog server.
7. In **Server IP/FQDN**, type the FQDN or IP address of the remote syslog server.
8. Click **Submit**.

Configuring log retention period

About this task

Use the Server Log Files page to configure the retention period and log file size for storing the logs that contain privacy-related data.

You can configure log retention for the following log types:

- Command History
- CM logs/MST Trace
- Linux Messages
- CDR Logs

You can configure Command History, CM Logs/MST Trace, and Linux Messages log types using Communication Manager SMI, and CDR logs using Communication Manager SAT interface. For more information on CDR logs, see *Avaya Aura® Communication Manager Screen Reference* guide.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, under **Security**, click **Server Log Files**.
4. In the **Log Retention Period** section, do the following:
   a. In the **Days** field, enter the number of days for which you want to retain the logs.
   b. In the **Capacity** field, enter the size of the logs in MB that you want to retain for each log type.
5. Click **Submit**.

6. **(Optional)** To push the log retention configuration to the ESS and LSP servers, go to Communication Manager SAT interface and run the following command: `save trans all`.

Station lock

Station Lock overview

Using the Station Lock feature, users can lock their telephones to prevent other callers from using their telephones.

To lock the phone, use a Feature Access Code (FAC) on an analog telephone.

On a digital telephone, use an FAC or a feature button.

Station Lock facilitates:

- Blocking of unauthorized outgoing calls
- Placing of outgoing emergency calls
- Receiving incoming calls

The feature button will light when the user will press the button to activate Station Lock. When a user attempts to place a call, the system generates a special dial tone to indicate that the Station Lock feature is active.

H.323 or DCP phones support the Station Lock functionality of Communication Manager. SIP phones do not support the functionality.

If a digital or an IP telephone has a **Station Lock** button, but uses an FAC to activate the feature, the system generates the special tone. If a digital or an IP telephone has a **Station Lock** button and uses this button to activate the feature, the system generates the special tone too. If a digital or an IP telephone does not have a **Station Lock** button and uses an FAC to activate the feature, the system generates the special tone.

On a digital telephone, use a **Station Lock** button instead of an FAC to activate Station Lock.

Any user who knows the systemwide FAC for Station Lock and the Station Security Code (SSC) of a specific telephone can lock or unlock the telephone.

A user can also lock or unlock a telephone from a remote location.

The attendant console can lock or unlock other telephones. The attendant console cannot be locked.

Preparing to set up Station Lock

Procedure

Be sure the **Station Lock COR** field on the Class of Restriction screen has the COR that the user is using to define the calling restrictions.

Setting up Station Lock with a Station Lock button example

About this task

We will set Station Lock to allow authorized users to access the system through a particular station (extension 7262).

Procedure

1. Enter `change station 7262`.
2. In the **Security Code** field, enter a security code of up to 8 digits.

   In the **COR** field, leave the default at `1`.
3. In the **BUTTON ASSIGNMENTS** section, type `sta-lock`.
4. Select `Enter` to save your changes.
5. Type **`change cor 1`** and press `Enter`.
6. In the **Calling Party Restriction** field, type `none`.

   This means that no calling party restrictions exist on extension 7262.
7. In the **Station Lock COR** field, type `2`.
8. Select `Enter` to save your changes.
9. Type **`change cor 2`** and press `Enter`.
10. In the **Calling Party Restriction** field, verify it is `outward`.
11. Select `Enter` to save your changes.

    Now when extension 7262 activates Station Lock, calling restrictions are determined by the Station Lock COR, COR 2. Based on the administration of COR 2, extension 7262 is disallowed to call outside the private network. When Station Lock is inactive on extension 7262, calling restrictions are determined by the COR administered on the Station screen, COR 1. In this example, when extension 7262 is unlocked, calls outside the private network are allowed.

Setting up Station Lock without a Station Lock button example

About this task

To set Station Lock on an analog, x-mobile, or digital telephone without a Station Lock button (extension 7262 and use a feature access code of 08):

Procedure

1. Enter `change station 7262`.
2. In the **Security Code** field, enter a security code of up to 8 digits.

   In the **COR** field, leave the default at `1`. This means that anyone can call outside on extension 7262.

3. Select `Enter` to save your changes.
4. Enter `change system-parameters features`.
5. In the **Special Dial Tone** field, type `y` for an audible tone indicating the station is locked.
6. Press `Enter` to save your changes.
7. Type **`change feature-access-codes`** and press `Enter`.
8. Move the cursor to the **Station Lock Activation** field.
9. In the **Activation** field, type `*08`.
10. In the **Deactivation** field, enter `#08`.
11. Select**Enter** to save your changes.

    Now when a user activates Station Lock, no one can call outside from extension 7262.

Station Lock by time of day

With Communication Manager 4.0 and later, you can lock stations using a Time of Day (TOD) schedule.

To engage the TOD station lock or unlock, you do not have to dial the station lock or unlock FAC.

When the TOD feature activates the automatic station lock, the station uses the COR assigned to the station lock feature for call processing. The COR used is the same for manual station locks.

The TOD lock or 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 and the station invokes a transaction which is denied by the Station Lock COR, the system displays Time of Day Station Locked. Whenever the station is within a TOD Lock interval and the special dial tone is administered, the user hears a special dial tone instead of the normal dial tone.
- 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 the special dial tone when the station is off hook.

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

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

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

The TOD feature does not unlock a manually locked station.

Note:

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

Screens for administering Station Lock

Screen name	Purpose	Fields
COR	Administer a COR for the user to activate Station Lock with an FAC.	**Station Lock COR**
Feature Access Code (FAC)	Assign an FAC for Station Lock activation, and another FAC for Station Lock Deactivation.	**Station Lock Activation** Station Lock Deactivation
Station	Assign the user a COR 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**
Feature Related System Parameters	Enable special dial tone.	**Special Dial Tone**

Security Violations responses

When a security violation occurs, there are steps that you can take to be sure that this same attempt is unsuccessful in the future.

Enabling remote access

About this task

You may have to enable Remote Access that has been disabled following a security violation, or disabled manually.

Procedure

1. Log in to Communication Manager using a login ID with the correct permissions.
2. Enter `enable remote-access`.

Disabling remote access

About this task

There might be occasions when you have to disable remote access for one of your users because of a security violation.

Procedure

1. Log in to Communication Manager using a login ID with the correct permissions.
2. Enter disable remote-access.

Hot Desking Enhancement

Hot Desking is a generic term for features that help 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 and 96x1 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 and 96x1 series H.323 IP telephones with the appropriate firmware change support the full range of HDE. The **Hot Desking Enhancement Station Lock** field is available on page 3 of the Feature-Related System Parameters screen.

Hot Desking interaction with PSA

The Hot Desking Enhancement (HDE) feature displays PSA Login information. You can invoke Personal Station Access (PSA) using H.323 IP telephones. If the Hot Desking Enhancement is activated, the telephone displays a text message to inform you how to log in again after PSA logoff. The message is sent to all telephones, including IP (H.323) telephones, if the **Hot Desking Enhancement Station Lock** field on the Feature-Related System Parameters screen is set to y.

Note:

The message is not sent to H.323 telephones on PSA Logoff. If an H.323 telephone is in state PSA Logoff and IP Login is used instead of PSA Login the display text of SA8582 is shown after going off hook or on hook. After dialing the FAC for PSA Login the text disappears.

The message used for displaying the PSA Login information is a non-call associated message, which gets shown at the top of an IP (H.323) telephone.

The **Hot Desking Enhancement Station Lock** field on the System-Parameters Features screen controls the feature.

Station Lock

Use the Station Lock feature to lock a telephone to prevent others from placing outgoing calls from the telephone.

Hot Desking with Station Lock restrictions

Parts of the Hot Desking Enhancement (HDE) feature apply only to telephones with firmware changes, while other parts apply to all telephones. The table here provides an overview.
For information on firmware vintage number, go to the Avaya Support website at http://support.avaya.com.

HDE Feature	96xx and 96x1 H.323 with FW changes	96xx and 96x1 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 14: Data Encryption

Note:

From Release 8.1.2, Avaya Aura® applications support the file system data encryption feature. This requires a new encryption capable variant of Release 8.1E OVA as prerequisite. The encryption can be enabled only at the time of deploying Avaya Aura® application 8.1E OVA. If you want to execute data encryption commands, then you must deploy Release 8.1E OVA and then apply Release 8.1.2 or later patch on it.

For more information on the encryption commands, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

From Release 8.1.2, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized Environment. Once you deploy the application with data encryption, you cannot disable data encryption after deployment.

In a software-only environment, the customer must enable the encryption at the operating system (OS) level. To be Data Privacy compliant, the customer must first encrypt the OS and apply the Release 8.1.2 or later patch.

For Data Privacy configuration, the software-only customer has the ability to protect data-in-transit, by utilizing the configuration to specify that TLS connections will be used in all situations like signaling, control, and log transport. Communication Manager Release 8.1.2 provides some further enhancements for TLS coverage to include CDR streaming and Communication Manager-to-CMS control channel.

For Data Privacy configuration for log retention, the software-only customer has the ability to deploy Release 8.1.2 features.

By enabling Data Encryption, your Communication Product's certain Operational data and Log Files will be encrypted. You will be prompted to enter a passphrase that will be used to create or access an encryption key. You must remember the encryption passphrase, if not it can result in locking up the system. Secondly, you will be asked to configure the option for local key storage.

It is important to note that the encryption of the disk may have a performance impact. For further information, refer to the Avaya Product Administration guide(s). Before you select an encryption option, please read the Data Privacy Guideline so that you may better understand these options.

By disabling Data Encryption, your Communication Product's Operational data and Log Files will not be stored in encrypted partitions.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is selected, you need to reenter the encryption passphrase whenever the application reboots.

During reboot, the application prompts you to enter the encryption passphrase on VM console at first boot and upon entering the correct encryption passphrase, the system mounts all the encrypted disks.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is not selected during OVA deployment, the application creates the Local Key Store and the system does not prompt you to type the encryption passphrase whenever the application reboots to mount the encrypted disks. You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application.

The following users can run the data encryption commands:

- Customer defined privileged account
- Any profile 18 user
- Root user

Encryption of Communication Manager partitions

When you enable data encryption for Communication Manager, the system encrypts the following partitions that have personal data.

- `/var/home`
- `/var/log`
- `/var/log/audit`
- `/var/xln`

Remote Key Server

When you enable data encryption for an application, you can set up remote key server. You can add multiple remote key servers. When you add a remote key server for the first time, the application disables the local key store. You can enable the local key store again after adding a remote key server. However, it is not recommended to enable local key store when the remote key server configuration exists.

If there is only one empty slot, then you cannot add a new remote key server or a new passphrase. The last empty slot is a “reserved” slot and you can use that only for changing the passphrase.

Application checks for the remote key server accessibility every 15 minutes. If any of the remote key server goes down, the application generates a Warning alarm. If all remote key servers are not accessible, then the application generates a Minor alarm.

Data Encryption password policy

The encryption passphrase must meet the following requirements:

- Must contain at least eight characters.
- Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.

Ensure that you keep the encryption passphrase safe. You need the encryption passphrase later.

Data encryption commands

The following CLI commands are available to make changes to the data encryption settings.

encryptionPassphrase command

Using the **encryptionPassphrase** command you can manage the encryption passphrase after deploying the application.

Syntax

```
encryptionPassphrase [add | change | remove | list]
```

add	Displays the prompts to add the encryption passphrase.
change	Displays the prompts to change the encryption passphrase.
remove	Removes the encryption passphrase.
list	Displays the encryption passphrase and slot assignment.

Considerations

You must deploy the application with data encryption.

Adding encryption passphrase

About this task

Use the **encryptionPassphrase add** command to add encryption passphrase.

You can add a maximum of seven encryption passphrases, if free slots are available.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase add**.
3. In **Enter existing passphrase**, type the encryption passphrase.
4. In **Enter new Passphrase**, type the new encryption passphrase.

5. In **Retype Passphrase**, retype the encryption passphrase.

Changing encryption passphrase

About this task

Use the **encryptionPassphrase change** command to change the existing encryption passphrase.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase change**.
3. At the prompt, in **Current Passphrase**, type the encryption passphrase.
4. In **Enter new Passphrase**, type the new encryption passphrase.
5. In **Retype Passphrase**, retype the encryption passphrase.

   The application displays the following message.

   ```
   Passphrase successfully changed.
   ```

Displaying encryption passphrase and slot assignment

About this task

Use the **encryptionPassphrase list** command to list the slots assignment, encryption passphrase, and remote server details.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase list**.

   The application displays the details based on the system configuration.

   ```
   Slot        Status      Passphrase/Remote Server
   ------------------------------------------------
   Key Slot 0: ENABLED     Passphrase
   Key Slot 1: ENABLED     Passphrase
   Key Slot 2: ENABLED     Passphrase
   Key Slot 3: ENABLED     Passphrase
   Key Slot 4: ENABLED     Passphrase
   Key Slot 5: Disabled    empty
   Key Slot 6: Disabled    empty
   Key Slot 7: Disabled    empty
   ```

   If key slots 0 to 6 are full, then key slot 7 will be Reserved.

Removing encryption passphrase

About this task

Use the **encryptionPassphrase remove** command to remove the existing encryption passphrase. You cannot remove all encryption passphrases, the application retains minimum one encryption passphrase.

If you attempt to delete the last encryption passphrase, the system displays the following message:

```
The last passphrase cannot be removed!
```

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase remove**.
3. At the prompt, in **Passphrase to remove**, type the existing encryption passphrase.

   The application displays the following message.

   ```
   Passphrase successfully removed.
   ```

encryptionRemoteKey command

Using the **encryptionRemoteKey** command you can manage the remote key server after deploying the application.

Syntax

```
encryptionRemoteKey [add | remove | list]
```

add	Displays the prompts to add the remote key server.
remove	Removes the remote key server.
list	Displays the remote key server and slot assignment.

Considerations

You must deploy the application with data encryption.

Adding remote key server

Before you begin

Ensure that the remote key server is configured and accessible.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey add** <Address> <Port>.

   Where:

   Address is the IP address or FQDN of the remote key server.

   Port is the port number of the remote key server. If you do not enter the port number the application uses the value of default port as 80.
3. In **Enter existing passphrase**, type the existing encryption passphrase.

   If the remote key server is not configured, the application displays the following message.

```
Remote key server not found
```

If the remote key server is configured, the application adds the remote key server. When you add a remote key server for the first time, the application disables the local key store.

Removing remote key server

About this task

Use the **encryptionRemoteKey remove** command to remove the existing remote key server.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey remove** <Address>.

   Where:

   Address is the IP address or FQDN of the remote key server.

   You must use the same IP address or FQDN value that you used to add the remote key server.
3. In **Passphrase**, type the existing encryption passphrase.

   The application removes the remote key server and displays the following message:

   ```
   RemoteKey successfully removed.
   ```

Displaying remote key server and slot assignment

About this task

Use the **encryptionRemoteKey list** command to list the slots assignment, encryption passphrase, and remote server details.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey list**.

   The application displays the details based on the system configuration.

```
Slot        Status      Passphrase/Remote Server
-----------------------------------------------
Key Slot 0: ENABLED     Passphrase
Key Slot 1: ENABLED     <IP Address of Remote Key Server>
Key Slot 2: ENABLED     Passphrase
Key Slot 3: DISABLED    empty
Key Slot 4: DISABLED    empty
Key Slot 5: DISABLED    empty
Key Slot 6: DISABLED    empty
Key Slot 7: DISABLED    empty
```

encryptionLocalKey command

Using the **encryptionLocalKey** command you can enable or disable the local key store after deploying the application with data encryption.

Syntax

```
encryptionLocalKey [enable | disable]
```

enable	Enables the local key store.
disable	Disables the local key store.

Considerations

You must deploy the application with data encryption.

Enabling local key store

About this task

Use the **encryptionLocalKey enable** command to enable the local key store.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionLocalKey enable**.
3. At the prompt, in **Enter existing passphrase**, type the existing encryption passphrase.

   If the local key store is already enabled, the application displays the following message.

   ```
   Local key store is already enabled.
   ```

Disabling local key store

About this task

Use the **encryptionLocalKey disable** command to disable the local key store.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionLocalKey disable**.

   The application displays the following message.

   ```
   Local keystore removed
   Local Key Store is now disabled.
   ```

Viewing data encryption status

About this task

The **encryptionStatus** command displays information about encryption on the system.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type `encryptionStatus`.
3. When the system prompts, type the password.

   For example, if the local key store is configured, the system displays the following status:

   ```
   Data Encryption: enabled
   Local Key Store: enabled
   Encryption Passphrase Required at Boot-time: no
   ```

   For example, if the remote key server is configured, the system displays the following status:

   ```
   Data Encryption: enabled
   Local Key Store: disabled
   Encryption Passphrase Required at Boot-time: yes
   remoteKeyServers: <remoteServer1: <remoteServerIPAddress> accessible>
   ```

Chapter 15: Managing Trunks

Tips for working with trunk groups

You'll find detailed procedures for administering specific trunk groups elsewhere in this chapter. However, there's more to working with trunks than just administering trunk groups.

Following a process when working with trunk groups

About this task

Trunking technology is complex. Following a process can prevent mistakes and save you time. Avaya recommends following the process below (some steps might not apply to your situation) to set up new trunks and trunk groups,:

Procedure

1. Install the necessary circuit packs and perform any administration the circuit pack requires.
2. Connect the appropriate ports to your network service provider's trunks.
3. Administer a trunk group to control the operation of the trunks.
4. Assign the ports you're using to the trunk group.
5. For outgoing or 2-way trunks, administer Automatic Route Selection so Communication Manager knows which outgoing calls to route over this trunk group.
6. Test your new trunk group by placing a variety of call using the trunk access code.

   Using the trunk access code, place a variety of calls.

   See Modifying Call Routing for detailed information on Automatic Route Selection.

Service provider coordination for trunk groups

Depending on the type of trunk you want to add, the vendor might be your local telephone company, a long distance provider, or some other service provider. Key settings on Communication Manager must be identical to the same settings on the provider's equipment for your trunks to work. Clear, frequent communication with your provider is essential — especially since some providers might use different terms and acronyms than Avaya does!

Once you decide that you want to add a new trunk, contact your vendor. The vendor should confirm the type of signal you want and provide you with a circuit identification number for the new

trunk. Be sure to record any vendor-specific ID numbers or specifications in case you ever have any problems with this trunk.

Records keeping for trunk groups

In addition to recording vendor-specific information such as ID numbers, you should record the following information about every trunk group you have.

The questions you need to answer	The kind of information you need to get
What type of trunk group is it?	You need to know what kind of trunks these are (central office (CO), foreign exchange (FX), and so on.) and whether they use any special services (such as T1 digital service). You also need to know what kind of signaling the group uses. For example, you might have a CO trunk group with ground-start signaling running on a robbed-bit T1 service.
Which telephone numbers are associated with each trunk group?	For incoming or two-way trunk groups: 1. What number or numbers do outside callers use to call into your server over this group? 2. What is the destination extension to which this trunk group delivers calls? Does it terminate at an attendant or a voice-mail system? For outgoing trunk groups: • What extensions can call out over this trunk group?
Is the service from your network service provider sending digits on incoming calls?	Direct Inward Dial and Direct Inward/Outward Dial trunks send digits to Communication Manager. Tie trunks can send digits, depending on how they're administered. You need to know: • How many digits is your service provider sending? • Are you inserting any digits? What are they? • Are you absorbing any digits? How many? • What range of numbers has your service provider assigned you?

Helpful tips for setting common trunk group fields

The procedures in this section cover the specific fields you must administer when you create each type of trunk group. Here are some tips for working with common fields that are available for most trunk groups.

- Dial Access — Type `y` in this field 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 need. For security, you might want to leave the field set to `n` unless you need dial access to test the trunk group.

- Outgoing Display — Type `y` in this field so that the display telephones can show the name and group number of the trunk group used for an outgoing call. This information might be useful to you when you're trying to diagnose trunking problems.
- Queue Length — Don't create a queue for two-way loop-start trunks, or you might have a problem with glare (the interference that happens when a two-way trunk is seized simultaneously at both ends).
- Trunk Type — Use ground-start signaling for two-way trunks whenever possible: ground-start signaling avoids glare and provides answer supervision from the far end. Try to use loop-start signaling only for one-way trunks.

Trunk group related information

See the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207, for information on the types of circuit packs available and their capacities.

See your server's Installation manual for circuit-pack installation instructions.

CO, FX, or WATS trunk group administration

Basic administration for Central Office (CO), Foreign Exchange (FX), and WATS trunk groups is identical, so we've combined instructions for all 3 in the following procedure. In most cases, Avaya recommends leaving the default settings in fields that aren't specifically mentioned in the following instructions. Go to the Avaya Support website at http://support.avaya.com for more information. Your settings in the following fields must match your provider's settings:

- Direction
- Comm Type
- Trunk Type

Caution:

Use the list above as a starting point and talk to your service provider. Depending on your particular application, you might need to coordinate additional administration with your service provider.

Preparing to add a CO, FX, or WATS trunk group

Procedure

Before you administer any trunk group, verify you have one or more circuit packs of the correct type with enough open ports to handle the number of trunks you need to add.

To find out what circuit packs you need, see the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Adding a CO, FX, or WATS trunk group example

About this task

As an example, we will set up a two-way CO trunk group that carries voice and voice-grade data only. Incoming calls terminate to an attendant during business hours and to a night service destination the rest of the time. We're adding trunk group 5 as an example.

Procedure

1. Enter **`add trunk-group next`**.
2. In the **Group Type** field, type `co`.

   This field specifies the kind of trunk group you're creating.
3. In the **Group Name** field, enter `Outside calls`.

   This name will be displayed, along with the group number, for outgoing calls if you set the **Outgoing Display** field to `y`. You can type any name up to 27 characters long in this field.
4. In the **COR** field, enter `85`.

   This field controls which users can make and receive calls over this trunk group. Assign a class of restriction that's appropriate for the COR calling permissions administered on your system.
5. In the **TAC** field, enter`105`.

   This field defines a unique code that you or your users can dial to access this trunk group. The code also identifies this trunk group in call detail reports.
6. In the **Direction** field, enter `two-way`.

   This field defines the direction of traffic flow on this trunk group.
7. In the **Night Service** field, enter `1234`.

   This field assigns an extension to which calls are routed outside of business hours.
8. In the **Incoming Destination** field, enter`attd`.

   This field assigns an extension to which incoming calls are routed during business hours. By entering attd in this field, incoming calls go to the attendant and the system treats the calls as Listed Directory Number calls.
9. In the **Comm Type** field, enter `voice`.

This field defines whether a trunk group can carry voice, data, or both. Analog trunks only carry voice and voice-grade data.

10. In the **Trunk Type** field, enter `ground-start`.

    This field tells the system what kind of signaling to use on this trunk group. To prevent glare, Avaya recommends ground start signaling for most two-way CO, FX, and WATS trunk groups.

11. Press **Next Page** until you find the **Outgoing Dial Type** field.
12. In the **Outgoing Dial Type** field, enter `tone`.

    This field tells Communication Manager how digits are to be transmitted for outgoing calls. Entering tone actually allows the trunk group to support both dual-tone multifrequency (DTMF) and rotary signals, so Avaya recommends that you always put tone in this field.

13. In the **Trunk Termination** field, enter `rc`.

    Use `rc` in this field when the distance to the central office or the server at the other end of the trunk is more than 3,000 feet. If you do not know the distance to your central office, check with your service provider.

14. Select `Enter` to save your changes.

    Now you are ready to add trunks to this trunk group. See Adding trunks to a trunk group example.

DID trunk group administration

In most cases, Avaya recommends leaving the default settings in fields that aren't specifically mentioned in the following instructions. Go to the Avaya Support website at http://support.avaya.com for more information. For Direct Inward Dialing (DID) trunk groups, settings in the following fields *must* match your provider's settings:

- Direction
- Comm Type
- Trunk Type
- Expected Digits (only if the digits your provider sends do not match your dial plan)

Caution:

Use the list above as a starting point and talk to your service provider. Depending on your particular application, you might need to coordinate additional administration with your service provider.

Preparing to add a DID trunk group

Procedure

Before you administer any trunk group, verify you have one or more circuit packs of the correct type with enough open ports to handle the number of trunks you need to add.

To find out what circuit packs you need, see the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Tip:

In the **DID/Tie/ISDN Intercept Treatment** field on the Feature-Related System Parameters screen, enter `attd`. Incoming calls to invalid extensions will be routed to the attendant.

Adding a DID trunk group example

Procedure

1. Enter **`add trunk-group next`**.

   The system assigns the next available trunk group number to this group. In our example, we're adding trunk group 5.

2. In the **Group Type** field, enter`did`.

   This field specifies the kind of trunk group you're creating.

3. In the **Group Name** field, enter `Incoming calls`.

   You can type any name up to 27 characters long in this field.

4. In the **COR** field, enter `85`.

   This field controls which users can receive calls over this trunk group. Assign a class of restriction that's appropriate for the COR calling permissions administered on your system.

5. In the **TAC** field, enter `105`.

   This code identifies the trunk group on CDR reports.

6. In the **Trunk Type** field, type wink-start.

   This field tells the system what kind of signaling to use on this trunk group. In most situations, use wink start for DID trunks to minimize the chance of losing any of the incoming digit string.

7. In the **Incoming Dial Type** field, enter `tone`.

   This field tells Communication Manager how digits are transmitted for incoming calls. Entering tone actually allows the trunk group to support both DTMF and rotary signals, so Avaya recommends that you always put tone in this field.

8. In the **Trunk Termination** field, enter`rc`.

Use `rc` in this field when the distance to the central office or the server at the other end of the trunk is more than 3,000 feet. If you do not know the distance to your central office, check with your service provider.

9. Select `Enter` to save your changes.

   Now you're ready to add trunks to this trunk group. See Adding trunks to a trunk group example.

   See Digit insertion and absorption with trunk groups for instructions on matching modifying incoming digit strings to match your dial plan.

PCOL trunk group administration

In most cases, when administering Personal Central Office Line (PCOL) trunk groups, Avaya recommends leaving the default settings in fields that aren't specifically mentioned in the following instructions. Go to the Avaya Support website at http://support.avaya.com for more information. Your settings in the following fields must match your provider's settings:

- Trunk Type
- Trunk Direction

Caution:

Use the list above as a starting point and talk to your service provider. Depending on your particular application, you might need to coordinate additional administration with your service provider.

Preparing to add a PCOL trunk group

Procedure

Before you administer any trunk group, verify you have one or more circuit packs of the correct type with enough open ports to handle the number of trunks you need to add.

To find out what circuit packs you need, see the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Adding a PCOL trunk group example

About this task

As an example, we will set up a new PCOL group and administer the group as a CO trunk for two-way voice traffic.

Procedure

1. Enter **`add personal-co-line next`**.
2. In the `Group Type` field, enter `co`.

This field specifies the kind of trunk group you're creating. PCOL groups can be administered as CO, FX, or WATS trunks.

3. In the **Group Name** field, enter `Outside calls`.

   This name will be displayed, along with the group number, for outgoing calls if you set the **Outgoing Display** field to `y`. You can type any name up to 27 characters long in this field. (You might want to put the telephone number here that's assigned to this trunk.)

4. In the **TAC** field, enter **111**.

   This field defines a unique code that you or your users can dial to access this trunk group. The code also identifies this trunk group in call detail reports.

5. In the **Trunk Type** field, enter `ground start`.

   This field tells the system what kind of signaling to use on this trunk group. To prevent glare, Avaya recommends ground start signaling for most two-way CO, FX, and WATS trunk groups.

6. In the **Trunk Port** field, enter `01D1901`.

   This is the port to which the trunk is connected.

7. In the **Trunk Termination** field, enter `rc`.

   Use `rc` in this field when the distance to the central office or the server at the other end of the trunk is more than 3,000 feet. If you do not know the distance to your central office, check with your service provider.

8. In the **Outgoing Dial Type** field, enter `tone`.

   This field tells Communication Manager how digits are to be transmitted for outgoing calls. Entering tone actually allows the trunk group to support both DTMF and rotary signals, so Avaya recommends that you always put tone in this field.

9. Select `Enter` to save your changes.

   You assign telephones to a PCOL group by administering a CO Line button on each telephone. Once assigned, the Assigned Members page of the Personal CO Line Group screen displays member telephones:

PCOL trunk group interactions

Call Detail Recording PCOL interaction

Call detail recording (CDR) can be activated for calls on a personal CO line, but the CDR record does not specifically identify the call as PCOL. Calls over personal CO lines can, however, be identified by the trunk access code used on the call. The call is recorded to the extension number assigned to the telephone where the call was originated or answered.

PCOL restrictions

- Abbreviated Dialing can be used with a personal CO line, but the accessed lists are associated with the individual telephones.
- Auto Hold and Leave Word Calling do not work with calls on a personal CO line.
- Send All Calls cannot be activated for a personal CO line.
- Avaya Aura® Messaging and Avaya 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 or idle status of the line.

Tie or Access trunk group administration

In most cases, Avaya recommends leaving the default settings in fields that aren't specifically mentioned in the following instructions. Go to the Avaya Support website at http://support.avaya.com for more information. Your settings in the following fields must match your provider's settings (or the setting on the far-end server, if this is a private network trunk group):

- Direction
- Comm Type
- Trunk Type

Caution:

Use the list above as a starting point and talk to your service provider. Depending on your particular application, you might need to coordinate additional administration with your service provider.

Preparing to add a Tie or Access trunk group

Procedure

Before you administer any trunk group, verify you have one or more circuit packs of the correct type with enough open ports to handle the number of trunks you need to add.

For more information about circuit pack, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Tip:

In the **DID/Tie/ISDN Intercept Treatment** field on the Feature-Related System Parameters screen, enter `attd`. Incoming calls to invalid extensions get routed to the attendant.

Adding a Tie or Access trunk group example

About this task

As an example, we will add a two-way tie trunk group that supports voice and voice-grade data. We're adding trunk group 5.

Procedure

1. Enter `add trunk-group next`.
2. In the **Group Type** field, enter `tie`.

   This field specifies the kind of trunk group you're creating.
3. In the **Groncup Name** field, enter `Outside calls`.

   This name will be displayed, along with the group number, for outgoing calls if you set the **Outgoing Display** field to `y`. You can type any name up to 27 characters long in this field.
4. In the **COR** field, enter `85`.

   This field controls which users can make or receive calls over this trunk group. Assign a class of restriction that's appropriate for the COR calling permissions administered on your system.
5. In the **TAC** field, enter `105`.

   This field defines a unique code users can dial to access this trunk group.
6. In the **Direction** field, enter `two-way`.

   This field defines the direction of traffic flow on this trunk group.
7. In the **Night Service** field, enter `1234`.

   This field assigns an extension to which calls are routed outside of business hours.
8. In the **Comm Type** field, enter `voice`.

   This field defines whether a trunk group can carry voice, data, or both. Analog trunks only carry voice and voice-grade data. If you're administering a T1 connection in North America, enter `rbavd` in this field.
9. In the **Trunk Type** field, enter `wink/wink`.

   This field tells the system what kind of signaling to use on this trunk group. Because we're receiving and sending digits over this trunk group, we're using wink/wink signaling to minimize the chance of losing part of the digit string in either direction.
10. Enter `tone` in both the **Outgoing Dial Type** and **Incoming Dial Type** fields.

    These fields tell Communication Manager how digits are transmitted for incoming calls. Entering tone actually allows the trunk group to support both DTMF and rotary signals, so Avaya recommends that you always put tone in this field.
11. Select `Enter` to save your changes.

Now you're ready to add trunks to this trunk group. See Adding trunks to a trunk group example.

DIOD trunk group administration

Administration for Direct Inward and Outward Dialing (DIOD) trunk groups varies from country to country. Go to the Avaya Support website at http://support.avaya.com for more information. Remember that the central office serving your switching system might be emulating another country's network protocol. If so, you'll have to administer your circuit packs and trunk groups to match the protocol used by your central office.

If you are using Incoming Caller ID (ICLID) on analog trunks connected to a DIOD Central Office trunk circuit pack, DO NOT put these trunks in an outgoing AAR or ARS route pattern. Since the loop-start trunks supported on the DIOD Central Office trunk circuit pack do not provide answer supervision, the potential for toll fraud exists.

Digital trunks administration

Any of the common trunks, except for PCOL trunks, can be analog or digital. (PCOL trunks can only be analog.) Administering a digital trunk group is very similar to administering its analog counterpart, but digital trunks must connect to a DS1 circuit pack and this circuit pack must be administered separately. The example in this section shows you how to do this.

In most cases, Avaya recommends leaving the default settings in fields that aren't specifically mentioned in the following instructions. Go to the Avaya Support website at http://support.avaya.com for more information.

Your settings in the following fields must match your provider's settings:

- Bit Rate
- Line Coding (unless you're using a channel service unit to convert between your line coding method and your provider's)
- Framing Mode
- Signaling Mode
- Interface Companding

⚠ Caution:

Use the list above as a starting point and talk to your service provider. Depending on your particular application, you might need to coordinate additional administration with your service provider.

See DS1 Circuit Pack in *Avaya Aura® Communication Manager Screen Reference* for information on administering DS1 service.

See DS1 Trunk Service in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information on DS1 service.

Preparing to add a digital trunk

Procedure

1. Assign the DS1 circuit pack before you administer the members of the associated trunk groups.

   Caution:

   If enhanced DS1 administration is disabled, you cannot make changes to the DS1 Circuit Pack screen before you remove related member translations of all trunks from the trunk group. See Enhanced DS1 administration.

2. Before you administer a digital trunk group, verify you have one or more circuit packs that support DS1 with enough open ports to handle the number of trunks you need to add.

   For more information about what circuit packs you need, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Setting up the DS1 board as a sync Source reference

Procedure

1. Enter `change ds1 n`, where *n* is the DS1 board location that you want to set up as a Sync Source.
2. Enter the necessary parameters to match the far end of the DS1 span.
3. Select **Enter** to save your changes.

Configuring a DS1 circuit pack example

About this task

The following example shows a DS1 circuit pack configured for T1 service. The circuit pack is supporting a two-way CO trunk group that carries only voice and voice-grade data.

To configure a new DS1 circuit pack:

Procedure

1. Enter **`add ds1 07A19`**.

   You must enter a specific port address for the circuit pack.

2. In the **Name** field, enter `two-way CO`.

   Use this name to record useful information such as the type of trunk group associated with this circuit pack or its destination.

3. In the **Bit Rate** field, enter `1.544`

   (Standard for T1 lines).

4. In the **Line Coding** field, enter `b8zs`.

   Avaya recommends you use `b8zs` whenever your service provider supports it. Since this trunk group only carries voice traffic, you could also use `ami-zcs` without a problem.

5. In the **Framing Mode** field, enter `esf`.

   Avaya recommends you use `esf` whenever your service provider supports it.

6. In the **Signaling Mode** field, enter `robbed-bit`.

7. In the **Interface Companding** field, enter `mulaw`.

   This is the standard for T1 lines in North America.

8. Select **Enter** to save your changes.

Recommended T1 and E1 settings

T1 recommended settings

The table below shows recommended settings for standard T1 connections to your local exchange carrier.

Field	Value	Notes
Line Coding	`b8zs`	Use `ami-zcs` if `b8zs` is unavailable.
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 unavailable.

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. Go to the Avaya Support website at http://support.avaya.com for more information.

Note:

Remember that the central office serving your switching system might be emulating another country's network protocol. If so, you'll have to administer your circuit packs and trunk groups to match the protocol used by your central office.

Enhanced DS1 administration

Normally, you can't change the DS1 Circuit Pack screen unless you remove all related trunks from their trunk group. However, if the **DS1 MSP** field on the System-Parameters Customer-Options

(Optional Features)screen is `y`, and you are assigned the associated login permissions, you can change some of the fields on the DS1 Circuit Pack screen without removing the related trunks from their trunk group.

If you busy out the DS1 circuit pack, you can change the following fields: **CRC**, **Connect**, **Country Protocol**, **Framing Mode**, **Interface**, **Interconnect**, **Line Coding**, and **Protocol Version**.

After changing these fields, you might also have to change and resubmit associated screens.

Enhanced DS1 administration matched field settings

For enhanced DS1 administration, some field values on the DS1 Circuit Pack screen must be consistent with those on other screens as shown in the table below. If you change field values on the DS1 Circuit Pack screen, you must change the related fields on the other screens and resubmit them.

DS1 Circuit Pack field	Affected screens[1]
Line Coding	Route Pattern
	Access Endpoint
	Signaling Group
	Tone Generation
Connect	Signaling Group
Protocol Version	Signaling Group
Interface	Signaling Group
Interconnect	Tone Generation
Country Protocol	Signaling Group
	Tone Generation

Specific combinations of settings for some of these fields are shown below.

ITC, Bit Rate, and Line Coding values for enhanced DS1 administration

The system displays **ITC (Information Transfer Capability)** field 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

[1] See *Avaya Aura® Communication Manager Screen Reference*

Interconnect and Group Type entries for enhanced DS1 administration

The system displays the **Interconnect** field on the DS1 Circuit Pack screen. The system displays the **Group Type** field 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

Adding trunks to a trunk group example

About this task

Use this procedure to add new trunks or to change the assignment of existing trunks. To change the assignment of existing trunks, remove them from their current trunk group and add them to the new group.

You must add a trunk group before you can assign and administer individual trunks. To add a new trunk group, see the instructions in this chapter for the type of group you want to add.

As an example, we will assign 5 trunks to a new tie trunk group, trunk group 5. We'll use ports on several circuit packs for members of this group.

Procedure

1. Enter `change trunk-group 5`.
2. Click **Next Page** to move to the Group Member Assignments screen.

   Some of the fields on this screen do not appear for every trunk group.
3. In the **Port** field in row 1, enter `1B1501`.

   This field assigns the first member of the trunk group to a port on a circuit pack.
4. In the **Name** field in row 1, enter `5211`.

   This is the extension assigned to this trunk. In general, type the circuit ID or telephone number for each trunk in this field. The information is helpful for tracking your system or troubleshooting problems. Update these fields whenever the information changes.
5. In the **Mode** field, enter `e&m`.

   Caution:

   An entry in this field is only required for some circuit packs. Dip switch settings on the circuit pack control the signalling mode used on the trunk group, so the entry in the Mode field must correspond to the actual setting on the circuit pack.
6. In the **Type** field, enter `t1-comp`.

   An entry in this field is only required for some circuit packs.

7. Repeat steps 3 to 6, as appropriate, for the remaining trunks.

   Notice that you can assign trunks in the same trunk group to ports on different circuit packs.

8. Select `Enter` to save your changes.

Removing trunk groups example

About this task

There's more to removing a trunk group than just executing the **`remove trunk-group`** command. If you're using Automatic Route Selection (ARS), you must remove an outgoing or two-way trunk group from any route patterns that use it. If you've administered **Trunk-Group Night Service** buttons for the trunk group on any telephones, those buttons must be removed or assigned to another trunk group.

As an example, we will remove trunk group 5. This two-way group is used in ARS route pattern 2. In addition, a **Trunk-Group Night Service** button on extension 8410 points to this group.

Procedure

1. In the Route Pattern screen for route pattern 2, clear the entries for trunk group 5.

   If you're replacing trunk group 5 with another trunk group, just type the information for the new trunk group over the old entries. Remember to press `Enter` to save your changes.

2. In the Station screen for extension 8410, clear the entry in the **BUTTON ASSIGNMENTS** field for the **Trunk-Group Night Service** button.
3. Select `Enter` to save your changes.
4. In the `Group Member Assignments` screen for trunk group 5, remove all member trunks from the group.

   See Adding trunks to a trunk group example for instructions.

5. Enter **`remove trunk-group 5`**.
6. Select `Enter` to remove the trunk group.

Trunk resets

To "reset" a trunk, use the **`busyout`** command followed by the **`release`** command, both executed in a SAT window. You can run these commands on a board, a port, a trunk group, or an individual trunk. The availability of these commands depends on your login permissions.

Note:

These commands can tear calls down, so use them with great caution. Go to the Avaya Support website at http://support.avaya.com for details.

Resetting a trunk group

Procedure

1. Enter `busyout trunk` **n**, where **n** is the number of the trunk group.
2. Enter **`release trunk`** **n**.

   The trunk group is reset. (Example: **`busyout trunk 43`** followed by **`release trunk 43`**.)

Resetting a trunk member

Procedure

1. Enter `busyout trunk` *n/x*, where *n* is the number of the trunk, and *x* is the trunk group member.
2. Enter `release trunk` **n/x**.

   The trunk group member is reset. (Example: **`busyout trunk 43/1`** followed by **`release trunk 43/1`**. Another example operation for an ISDN trunk is **`test trunk 43`**.)

Digit insertion and absorption with trunk groups

Use these procedures to modify the incoming digit string on DID and tie trunks by inserting (adding) or absorbing (deleting) digits. You'll need to do this if the number of digits you receive doesn't match your dial plan.

See DID trunk group administration for instructions on administering a DID trunk group.

See Tie or Access trunk group administration for instructions on administering a tie trunk group.

Inserting digits with trunk groups example

About this task

As an example, let us say you have a DID trunk group. It's group number is 5. Your service provider can only send 4 digits, but your dial plan defines 5-digit extensions beginning with 6:

Procedure

1. Enter `change trunk-group 5`.
2. In the **Digit Treatment** field, enter `insertion`.

This field tells Communication Manager to add digits to the incoming digit string. These digits are always added at the beginning of the string.

3. In the **Digits** field, enter `6`.

   For insertion, this field defines the specific digits to insert. Communication Manager will add a “6” to the front of the digit strings delivered with incoming calls. For example, if the central office delivers the string “4444,” Communication Manager will change it to “64444,” an extension that fits your dial plan.

4. In the Expected Digits field, enter `4`.

   This field tells Communication Manager how many digits the central office sends.

   Note:

   The **Expected Digits** field does not appear on the screen for tie trunk groups.

5. Select `Enter` to save your changes.

Absorbing digits with trunk groups example

About this task

If your service provider sends 7 digits but you only need 5, you need to absorb the first 2 digits in the digit string.

Procedure

1. Enter `change trunk-group 5`.
2. In the **Digit Treatment** field, enter `absorption`.

   This field tells Communication Manager to remove digits from the incoming digit string. These digits are always removed from the beginning of the string.

3. In the **Digits** field, enter `2`.

   For absorption, this field defines how many digits will be absorbed. Communication Manager will remove the first 2 digits from the digit strings delivered with incoming calls. For example, if the central office delivers the string “556-4444,” Communication Manager will change it to “64444,” an extension that fits your dial plan.

4. In the **Expected Digits** field, enter `7`.

   This field tells Communication Manager how many digits the central office sends.

   Note:

   The **Expected Digits** field does not appear on the screen for tie trunk groups.

5. Select `Enter` to save your changes.

Administering trunks for LDN example

About this task

Listed directory numbers (LDN) are the telephone numbers given for an organization in public telephone directories. You can administer Communication Manager so that calls to different listed directory numbers go to the same attendant group. How you administer your system for LDN calls depends on whether the calls are coming in over DID and tie trunks or over CO and FX trunks.

As an example, let us say that one attendant group answers calls for 3 different businesses, each with its own listed directory number:

Procedure

1. Company A — 855-2020
2. Company B — 855-1000
3. Company C — 855-1111

   DID trunks and some tie trunks transmit part or all of the dialed digit string to Communication Manager. If you want these calls to different numbers to go to one attendant group, you must identify those numbers for Communication Manager on the Listed Directory Numbers screen.

   We will take the 3 businesses listed above as an example. We will assume your server receives 4 digits from the central office on a DID trunk group and that you're not using Tenant Partitioning. To make these calls to different listed directory numbers terminate to your attendant group:

   a. Enter `change listed-directory-numbers`.
   b. In the **Ext 1** field, enter`2020`.

      This is the LDN for Company A.
   c. In the **Name** field, enter `Company A`.

      The system displays the name on the console display so the attendant knows which business the call is for and how to answer it.
   d. Repeat steps 2 and 3 for the other two businesses.

      You can enter up to 20 different listed directory numbers on this screen.
   e. Select `Enter` to save your changes.

   To make LDN calls over a CO or FX trunk group terminate to an attendant group, you must type attd in the **Incoming Destination** field on the Trunk Group 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.

   See Listed Directory Numbers in *Avaya Aura® Communication Manager Screen Reference* for detailed information about this feature.

Administering trunks for Source-based Routing

Before you begin

On the Trunk Group screen, ensure that the value of the **Group Type** field is sip.

About this task

Communication Manager uses the Source-based Routing feature to send the location information of H.323, DCP, and analog stations to Session Manager.

Procedure

1. In a SAT session, type `change trunk-group n`, where *n* is the number of the trunk group.
2. On the Protocol Variations screen, change the **Block Sending Calling Party Location in INVITE** field to `n`.
3. Save the changes and exit the screen.

Answer Detection Administration

Use this procedure to administer an outgoing or two-way trunk group for network answer supervision or answer supervision by timeout. If your network supplies answer supervision to a trunk group, you can administer Communication Manager to recognize and respond to that signal. If your network does not supply answer supervision, you can set a timer for all calls on that group. When the timer expires, Communication Manager assumes the call has been answered and call detail recording starts (if you are using CDR).

For information about answer detection by call classification, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Preparing to administer Answer Detection

Procedure

Determine whether the trunk group receives answer supervision from your service provider or private network.

For example, most loop-start CO, FX, and WATS trunks do not provide answer supervision.

Administering Answer Detection example

About this task

As an example, we will administer trunk group 5 for both types of answer detection.

Procedure

1. On the Trunk Group screen for group 5, enter `y` in the **Receive Answer Supervision** field.

2. Select `Enter` to save your change.

   Now we will administer answer supervision by timeout. We'll set the timer to 15 seconds.

   a. On the Trunk Group screen for group 5, type `15` in the **Answer Supervision Timeout** field.

   b. Select `Enter` to save your change.

   For more information about this feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

ISDN trunk groups Administration

Integrated Services Digital Network (ISDN) trunk groups support the ISDN and Call-by-Call Service Selection service selection features. The trunk group provides end-to-end digital connectivity and supports a wide range of services including voice and non-voice services, to which users have access by a limited set of CCITT-defined, standard multipurpose interfaces.

The ISDN trunk group can contain ISDN-PRI or ISDN-BRI interfaces. However, it is not possible to use the two types of interfaces in the same trunk groups. The type of interface is chosen when the trunk members are assigned to the trunk group.

When ISDN-PRI interfaces are used on ISDN trunk groups, they can also be used to support the Wideband Switching feature. This is intended to work with the H0 (384 Kbps), H11 (1536 Kbps), H12 (1920 Kbps), and NXDS0 (128 to 1984 Kbps) data services, and to support high-speed video conferencing and data applications.

When an ISDN trunk connects two servers or switches, set the trunk options identically at both ends of the connection, with the exception of the **Trunk Hunt** fields. When ISDN-PRI interfaces are used, it is acceptable for both ends to have the **Trunk Hunt** fields administered as cyclical, but if one end is administered as ascend, the other end must be administered as descend. This helps avoid the possibility of glare conditions. When ISDN-BRI is used, the **Trunk Hunt** field has to be cyclical.

ISDN trunk group hardware requirements

ISDN-BRI trunk interfaces are supported by all of these:

- The TN2185 Trunk-side BRI circuit pack and the MM722 BRI circuit pack implement the user side of the BRI trunk interface.
- The TN556B/C/D ISDN-BRI Line circuit pack and the TN2198 ISDN BRI (U-LT) Line circuit pack implement the network side of the BRI trunk interface.
- The MM720 BRI circuit pack implements both sides of the interface. You can select the options from the BRI Trunk Circuit Pack screen

For BRI trunk connections to a public ISDN, use the TN2185, MM722, or MM720. For BRI tie trunks between systems, use the TN2185, MM722, or MM720 on one side and the TN556B/C/D or TN2198 on the other side. The TN2464 circuit supports T1 and E1 digital facilities.

ISDN-PRI interfaces are supported by the TN767 circuit pack (for assignment of a T1 signaling link and up to 24 ISDN-PRI trunk group members), or the TN464C or later circuit pack (for assignment of a T1 or E1 signaling link and up to 24 or 31 ISDN-PRI trunk group members, respectively). The TN2464 and TN2207 circuit pack can also be used with ISDN-PRI.

- The D-channel for ISDN-PRI interfaces switches through either the TN765 Processor Interface (PI) circuit pack or the TN778 Packet Control (PACCON) circuit pack. The D-channel for ISDN-BRI interfaces only switches through the TN778 Packet Control (PACCON) circuit pack.

  Note:

  You cannot use the TN765 circuit pack with ISDN-BRI interfaces.

- A TN780 or TN2182 Tone Clock circuit pack provides synchronization for the DS1 circuit pack.

Note:

The TN767 cannot be used to carry the D-channel if either the TN778 (PACCON) or TN1655 (PKTINT) circuit packs are used to switch the D-channel. However, in these circumstances, the TN767 can be used for NFAS interfaces carrying only B-channels.

Screens used to administer ISDN trunk groups

Screen	Field
Feature-Related System Parameters	**Send Non-ISDN Trunk Group Name as Connected Name?** **Display Connected Name/Number for ISDN DCS Calls?**
Incoming Call Handling Treatment	All
Numbering - Public/Unknown Format	**All**
System Parameters Customer-Options (Optional Features)	**Version** **ISDN-BRI Trunks** **ISDN-PRI** **QSIG Optional Features**
Synchronization Plan	**All**
Trunk Group (ISDN)	**All**
ISDN-BRI Circuit Pack screen (if using ISDN-BRI interfaces) or DS1 Circuit Pack screen (if using ISDN-PRI interfaces)	**All** **All**
ISDN Numbering - Private	**All**
Route Pattern	**All**
Hunt Groups	**ISDN Caller Display**

Table continues…

Screen	Field
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, go to the Avaya Support website at http://support.avaya.com.
- **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 I**SDN 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 system displays the following error message: `You cannot mix BRI and PRI ports in the same trunk group.`

Administering displays for QSIG trunks

Procedure

1. On the Trunk Group screen set the following fields:
   - **Group Type**: ISDN
   - **Character Set for QSIG Names**: iso8859-1
   - **Outgoing Display**: y
   - **Send Calling Number**: y
2. On the Signaling Group screen set the following fields:
   - **Supplementary Service Protocol**: b
3. On the System-Parameters Country-Options screen set the following field:
   - **Display Character Set**: Roman

QSIG over SIP

Use the QSIG over SIP (Q-SIP) feature to enable calls between two Communication Manager systems interconnected by an IP network that uses SIP signaling with the full range of QSIG functionality.

Preparing to administer QSIG over SIP

Before you begin

Ensure that the system is running Communication Manager Release 6.0 or later. Release 6.0 or later is required on all nodes that participate in Q-SIP calls. The nodes can be originating, tandem, or terminating.

Procedure

1. Enter `display system-parameters customer-options`.
2. Click **Next** until you find the **Maximum Administered IP Trunks** field.
3. Ensure that the **Maximum Administered IP Trunks** field is set to greater than 1 and include enough trunks for Q-SIP trunk group use.
4. Click **Next** until you find the **Maximum Administered SIP Trunks** field.
5. Ensure that the **Maximum Administered SIP Trunks** field is set to greater than 1 and include enough trunks for Q-SIP trunk group use.
6. Scroll through the screens to find the **IP Trunks** field.
7. Ensure that the **IP Trunks** field is set to `y`.

Note:

If the **Maximum Administered IP Trunks** and **Maximum Administered SIP Trunks** fields are set to less than 1, or the **IP Trunks** field is set to n, your system is disabled for the QSIG over SIP feature. Go to the Avaya Support website at http://support.avaya.com for assistance.

8. Select **Enter** to exit the screen.

Administration of the QSIG and SIP trunk and signaling groups

You must administer the following trunks on each node:

- H.323 IP trunk equipped with QSIG signaling
- SIP trunk equipped with SIP signaling

You must administer the required number of QSIG and SIP trunk group members.

For information about creating the QSIG and SIP trunk and signaling groups, see *Administering Network Connectivity on Avaya Aura® Communication Manager*.

Note:

When creating the QSIG and SIP trunk groups, do not add trunk members to these trunk groups. Add the trunk members to the trunk groups after changing the QSIG and SIP trunk groups.

Note:

You must configure the Far-end Node Name of the QSIG signaling group, though the QSIG trunk serves as the feature layer and has no Far End. Due to the missing Far end, a dummy ip-node name must be used with the same IP address, which is already used for the Near End. You need to define this dummy ip-node name in the IP node name table before creating the QSIG signaling group.

Note:

If you create a new QSIG signaling group, must not use the default port 5060.

For Q-SIP you must specifically change the QSIG and SIP trunk and signaling groups. This is described in the following sections.

Enabling Enhanced SIP Signaling feature

Procedure

1. Type `display trunk-group n`, where *n* is the trunk group number.
2. On Protocol Variations page of the Trunk Group screen, ensure that the **Network Call Redirection** field is set to n for SIP trunks between Communication Manager and Session Manager.
3. Save the changes and exit the screen.

4. Type `change system-parameters features`. The system displays the Feature-related system parameters screen.
5. On page 19 of the Feature-related system parameters screen, set the **SIP Endpoint Managed Transfer** field to `y`.
6. Save the changes and exit the screen.

Changing the QSIG and SIP signaling groups for Q-SIP

Before you begin

Ensure that the QSIG and SIP signaling groups exist.

About this task

- Change the QSIG signaling group.
- Change the SIP signaling group.

Changing the QSIG signaling group

Procedure

1. Enter `change signaling-group n`, where *n* is the signaling group number, for example, *n* = 18.
2. Set the **Q-SIP** field to `y`.

   By default, the Q-SIP feature is disabled. The system displays this field only when the **Group Type** field is set to SIP or H.323.
3. In the **SIP Signaling Group** field, type a valid entry.

   The valid entry must refer to an administered SIP signaling group. For example, if you have created SIP signaling group 17, the **SIP Signaling Group** field must refer to SIP signaling group 17. The system displays this field only when the **Q-SIP** field is set to y.
4. Select **Enter** to save your changes.

Changing the SIP signaling group

Procedure

1. Enter `change signaling-group n`, where *n* is the signaling group number, for example, *n* = 17.
2. Set the **Q-SIP** field to `y`.

   By default, the Q-SIP feature is disabled. The system displays this field only when the **Group Type** field is set to SIP or H.323.
3. In the **QSIG Signaling Group** field, type a valid entry.

   The valid entry must refer to an administered H.323 signaling group. For example, if you have created QSIG signaling group 18, the **QSIG Signaling Group** field must refer to

QSIG signaling group 18. The system displays this field only when the **Q-SIP** field is set to y.

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

Changing the QSIG and SIP trunk groups for Q-SIP

Before you begin

Ensure that the QSIG and SIP trunk groups exist.

About this task

- Change the QSIG trunk group.
- Change the SIP trunk group.
- Add trunk group members to the QSIG trunk group.
- Add trunk group members to the SIP trunk group.

Changing the QSIG trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number, for example, *n* = 18.
2. Ensure that the **Group Type** field is `isdn` and **Carrier Medium** field is `H.323`.
3. Click **Next** until you see the QSIG Trunk Group Options section.
4. In the **SIP Reference Trunk Group** field, type a valid entry.

   The valid entry must refer to an administered SIP trunk group. For example, if you have created SIP trunk group 17, the **SIP Reference Trunk Group** field must refer to SIP trunk group 17.
5. Set the **TSC Method for Auto Callback** field to `drop-if-possible`.
6. Select **Enter** to save your changes.

Changing the SIP trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number, for example, *n* = 17.
2. Ensure that the **Group Type** field is set to `SIP`.
3. Click **Next** until you see the **Protocol Variations** section.
4. Set the **Enable Q-SIP** field to `y`.

   By default, the Q-SIP feature is disabled.
5. In the **QSIG Reference Trunk Group** field, type a valid entry.

   The valid entry must refer to an administered QSIG trunk group. For example, if you have created QSIG trunk group 18, the **QSIG Reference Trunk Group** field must refer to QSIG trunk group 18.

6. Select **Enter** to save your changes.

Adding trunk group members to the QSIG trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number, for example, *n* = 18.
2. Click **Next** until you see the Group Member Assignments section.
3. Add trunk group members to the numbered **Group Member Assignments**.
4. Select **Enter** to save your changes.

Note:

Instead of adding the trunk group members on the **Group Member Assignments**, you can set the **Member Assignment Method** field to `auto` and set the Number of Members.

Adding trunk group members to the SIP trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number, for example, *n* = 17.
2. Click **Next** until you see the Group Member Assignments section.
3. Add trunk group members to the numbered **Group Member Assignments**.
4. Select **Enter** to save your changes.

Note:

Instead of adding the trunk group members on the **Group Member Assignments**, you can set the Number of Members.

Routing of QSIG over SIP

Procedure

From the caller or calling party point of view, only the QSIG trunk is seen and used for routing, for example, in the route pattern. The SIP trunk is not seen and must not be used for routing.

Verifying a Q-SIP test connection

Procedure

1. Establish a Q-SIP call.
2. Type `status trunk QSIG-group-number`, where *QSIG-group-number* is the QSIG trunk group number in use.

   You must remember the active trunk group member for verifying a Q-SIP connection.

3. Type `status trunk QSIG-group-number/member-number`, where *QSIG-group-number* is the QSIG trunk group number and *member-number* is the QSIG trunk group member number, which you have identified in step 2. Press `Enter`.
4. On the Trunk Status screen, if a station is connected to a QSIG over SIP trunk, you can view the involved port of the QSIG trunk in the **Q-SIP Reference Port** field.
5. Type `status station n`, where *n* is the extension of the station.
6. On the General Status screen, if a station is connected to a QSIG over SIP trunk, you can view the involved port of the SIP trunk in the **Connected Ports** field. However, you cannot view the port of the QSIG trunk because the port is not involved in the media connection.

   See the description of the Connected Ports field in *Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers*, for more information.
7. Press `Enter` to exit the screen.

Removing the Q-SIP configuration

Disabling Q-SIP for the QSIG signaling group

Procedure

1. Enter `change signaling-group n`, where *n* is the signaling group number, for example, *n* = 18.
2. Set the **Q-SIP** field to `n`.
3. Select **Enter** to save your changes.

Disabling Q-SIP for the SIP signaling group

Procedure

1. Enter `change signaling-group n`, where *n* is the signaling group number, for example, *n* = 17.
2. Set the **Q-SIP** field to `n`.
3. Select **Enter** to save your changes.

Disabling Q-SIP for the QSIG trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number, for example, *n* = 18.
2. Click **Next** until you see the QSIG Trunk Group Options section.
3. Set the **SIP Reference Trunk Group** field to `blank`.
4. Select **Enter** to save your changes.

Disabling Q-SIP for the SIP trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the number of the trunk group number, for example, *n* = 17.
2. Click **Next** until you see the Protocol Variations section.
3. Set the **Enable Q-SIP** field to *n*.
4. Select **Enter** to save your changes.

Chapter 16: Managing media gateways

For details of hardware components, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

For more information about managing media gateways, see the following:

- *Administering Avaya G450 Branch Gateway*
- *Administering Avaya G430 Branch Gateway*
- *Avaya Branch Gateway G450 CLI Reference*
- *Avaya Branch Gateway G430 CLI Reference*
- *Avaya G450 Branch Gateway Overview and Specification*
- *Avaya G430 Branch Gateway Overview and Specification*

Chapter 17: Managing Avaya Aura® Media Server

Detailed description of Avaya Aura® Media Server (MS)

Avaya Aura® Media Server (MS) is used by Communication Manager to provide the following IP audio capabilities similar to the legacy H.248 media gateways or port networks with media processors:

- Termination of RTP audio streams
- Conferencing of RTP audio streams
- Playing and recording announcements
- Playing audio stream as an announcement
- Generation of system tones
- Digit collection

The Avaya Aura® Media Server (MS) instances and Avaya Aura® Media Server (MS) channels are licensed features. Each Avaya Aura® Media Server (MS) must obtain an instance license from a WebLM server. Avaya Aura® Media Server (MS) channels are licensed through the Communication Manager feature license file, which specifies the number of Avaya Aura® Media Server (MS) channels that are allowed on a specific Communication Manager. Avaya Aura® Media Server (MS) channels can be established on any Avaya Aura® Media Server (MS) configured on Communication Manager.

Avaya Aura® Media Server (MS) can provide different tones for locations that are configured on Communication Manager. When you enable the **Multinational Locations** feature on the system-parameters customer-options form, the VoIP selection algorithm considers Avaya Aura® Media Server (MS) as a Location Parameter Index (LPI) matching VoIP resource. Although endpoints LPI is different than the native LPI of Avaya Aura® Media Server (MS).

Avaya Aura® Media Server (MS), as a VoIP resource, can provide tones per user location. However, if more than one user is involved in a call from different locations, the system uses the Avaya Aura® Media Server (MS) native location that is configured on the SIP signaling group page.

For more information, see *Implementing and Administering Avaya Aura® Media Server* guide.

Related links

Administering Avaya Aura Media Server signaling group on Communication Manager on page 366
Changing Avaya Aura Media Server signaling group on Communication Manager on page 367

Adding a media-server on page 368
Verifying that the media-server is in-service on page 369
Removing a media server on page 369

Administering Avaya Aura® Media Server signaling group on Communication Manager

About this task

Use the following task to add an Avaya Aura® Media Server (MS) signaling group.

Before you begin

Ensure that you have configured the node name of Avaya Aura® MSusing the **`change node-names ip`** command.

For more information, see *Administering Avaya Aura® Communication Manager*.

Procedure

1. On the CLI, type the **`add signaling-group x`** command.
2. Press `Enter`.
3. On the SIGNALING GROUP screen, set **Group Type** to **SIP**.
4. Set **Transport Method** to one of the following:
   - `TCP`
   - `TLS`
5. Set **Peer Detection Enabled ?** to `n`.
6. Set **Peer Server** to `AMS`.
7. Set the node name of Avaya Aura® MS.
   - For TCP, the default value for both **Near-end Listen Port** and **Far-end Listen Port** is set at 5060. To use TCP as a Transport method, you must add Communication Manager as trusted node in the respective Avaya Aura® MS.
   - For TLS, the **Near-end Listen Port** default value is set at 9061, and the **Far-end Listen Port** is set at 5061.

Note:

- The **Far-end Node Name** can only contain a node name that has an IPv4 address. The system displays an error if the node name does not have an IPv4 address.
- The **Far-end Domain** is auto-populated and viewable as read-only with the IP address of the media server based on the **Far-end Node Name**.
- The **Near-end Node Name** is read-only and is auto-populated with the string procr.

```
change signaling-group 3                                    Page   1 of   2
                              SIGNALING GROUP
```

```
Group Number: 3              Group Type: sip
                       Transport Method: tls


  Peer Detection Enabled? n  Peer Server: AMS



   Near-end Node Name: procr                 Far-end Node Name: AMS
 Near-end Listen Port: 9061               Far-end Listen Port: 5061
                                    Far-end Network Region: 1

Far-end Domain: 172.30.32.49
```

Related links

Detailed description of Avaya Aura Media Server (MS) on page 365

Changing Avaya Aura® Media Server signaling group on Communication Manager

About this task

Use the task to change an Avaya Aura® Media Server (MS) signaling group.

Before you begin

Ensure that you have added the Avaya Aura® Media Server (MS) signaling group. For more information, see Administering Avaya Aura® Media Server on Communication Manager.

Procedure

1. On the CLI, type the **`change signaling-group`** x command, press `Enter`.

   By using the **`change signaling-group`** x command, you can add an IP node-name for the specific Avaya Aura® Media Server (MS) Signaling Group that you want to add.
2. On the SIGNALING GROUP screen, set **Group Type** to **SIP**.
3. Set **Transport Method** to one of the following:
   - `TCP`
   - `TLS`
4. Set **Peer Detection Enabled ?** to `n`.
5. Set **Peer Server** to `AMS`.
6. Set **Far-end Node Name** to the IPv4 address.
   - For TCP, the default value for both **Near-end Listen Port** and **Far-end Listen Port** is set at 5060.
   - For TLS, the **Near-end Listen Port** default value is set at 9061, and the **Far-end Listen Port** is set at 5061.

Note:

- The **Far-end Node Name** can only contain a node name that has an IPv4 address. The system displays an error if the node name has an IPv4 address.
- The **Far-end Domain** is auto-populated and viewable as read-only with the IP address of the media server based on the **Far-end Node Name**.
- The **Near-end Node Name** is read-only and is auto-populated with the string procr.

```
change signaling-group 10                                       Page   1 of   2
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
                        Transport Method: tls


  Peer Detection Enabled? n  Peer Server: AMS



   Near-end Node Name: procr                 Far-end Node Name: AMS-HA
 Near-end Listen Port: 9061               Far-end Listen Port: 5061
                                    Far-end Network Region: 3

Far-end Domain: 172.30.32.41
```

Related links

Detailed description of Avaya Aura Media Server (MS) on page 365

Adding a media-server

About this task

Use the task to add an Avaya Aura® Media Server (MS) media-server.

Before you begin

Ensure that you have added the Avaya Aura® Media Server (MS) signaling group. For more information, see Administering Avaya Aura® Media Server signaling group Communication Manager.

Procedure

1. Type the `add media-server xx` command.
2. On the MEDIA SERVER screen, in the **Signaling Group** field, type the signaling group of the Avaya Aura® Media Server (MS) signaling-group created in the Adding an Avaya Aura® Media Server (MS) signaling-group section.

```
add media-server 22                                             Page   1 of   1
                                MEDIA SERVER

                    Media Server ID: 22

                    Signaling Group:
          Voip Channel License Limit:
    Dedicated Voip Channel Licenses:
```

The **VoIP Channel License Limit** field can be left blank. Type the value if you want to limit the number of channels that can be established on the specified media-server. A blank field indicates that the channel limit is limited only by the physical capacity of the specific Avaya Aura® Media Server (MS).

The aggregate of dedicated channels administered across all media-servers must not exceed the number of licensed VoIP channels.

Related links

Detailed description of Avaya Aura Media Server (MS) on page 365

Verifying that the media-server is in-service

About this task

Use the task to verify that the media-server is operating.

Before you begin

Ensure that you have a licensed media server.

Procedure

On the CLI, type the **`status media-server`** `x` command, press `Enter`.

- Ensure that the **State** field displays in-service.
- The **Near-end Node Name** is read-only and is auto-populated with the string procr.

```
status media-server 2                                          Page   1 of   2
                            MEDIA SERVER STATUS


                  Media Server Number: 2
                                State: in-service
                    Signaling-group: 4
                          Node Name: AMSVM
                         IP Address: 172.30.32.37
                     Network Region: 1
                         SW-Version: 7.7.0.188
          Voip Channel License Limit:
      Dedicated Voip Channel Licenses:
         Voip Channel Licenses in-use: 0
                          Load Factor: 2
           Estimated Channel Capacity: 1492
                Announcements Present: 7
```

Related links

Detailed description of Avaya Aura Media Server (MS) on page 365

Removing a media server

Procedure

1. Remove all the announcements that point to the specific media-server.
2. Remove the specific media-server that must be removed from all the audio groups.

3. Remove the media-server from the media-server reporting lists on all the survivable-processor forms.

   The status media-server indicates the survivable-processors that is used by the media-server.

4. Busy out the signaling group that appears on the media-server form.
5. Run the **remove media-server** x command.

```
remove media-server 1                                          Page   1 of   1
                                MEDIA SERVER

                    Media Server ID: 1

                    Signaling Group: 1
         Voip Channel License Limit:
   Dedicated Voip Channel Licenses:

                         Node Name: AMS
                    Network Region: 5
                          Location: 2
          Announcement Storage Area: ANNC-00ac215c-fe5f-e401-5240-54545acc0000
```

Related links

Detailed description of Avaya Aura Media Server (MS) on page 365

Managing Avaya Aura® Media Server related documents

For more information about Avaya Aura® MS, see:

- *Avaya Aura® Communication Manager Screen Reference*
- *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*
- *Alarms and Performance Measurements for Avaya Aura® Media Server*
- *Implementing and Administering Avaya Aura® Media Server*
- *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*
- *Using Web Services on Avaya Aura® Media Server*
- *Deploying and Updating Avaya Aura® Media Server Appliance*
- *Overview for Avaya G430 Branch Gateway*
- *Overview for the Avaya G450 Media Gateway*
- *Administering Avaya G430 Branch Gateway*
- *Administering Avaya G450 Media Gateway*

- *Branch Gateway G430 Branch GatewayCLI Reference Guide*
- *Branch Gateway G450 Media Gateway CLI Reference Guide*

Chapter 18: Telephone announcements

An announcement is a recorded message that a caller can hear while the call is in a queue, or if the caller receives an intercept message for any reason. An announcement is often used in conjunction with music.

The source for announcements can be either integrated or external.

- Integrated announcements are integrated in a circuit pack in the carrier, such as the TN2501AP circuit pack or embedded in a gateway processor board. This board is called a vVAL source.
- 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 refer to integrated or external sources of announcements.

For information on music streaming from media server, see chapter “Music streaming configuration” of the document*Implementing and Administering Avaya Aura® Media Server*.

VAL or Gateway Virtual VAL resources

Before you can use the capabilities of the VAL or Gateway v VAL announcement circuit pack, it must be properly installed and configured. These instructions are contained in other documents in the Communication Manager documentation library.

- For a complete description of Announcement information and procedures, see the Announcements feature in *Avaya Aura® Communication Manager Feature Description and Implementation*.
- For a complete description of the related Locally Sourced Announcement feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*.
- 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*.

Table continues…

Task	Information source
Installing v VAL for a Gateway using the Media-Gateway screen and the **enable announcement** command Administering IP Connections Adding IP Routes Testing the IP Connections **Note:** 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 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, Branch Gateways and Servers*. Announcements can be administered to a gateway and files can be FTPed to that gateway even though it is disabled. However, the Gateway first must be assigned on the Media-Gateway screen so as to be used for gateway announcements. Each 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 Servers) if the **VAL Maximum Capacity** field is `y`. First the Gateway must have the **V9** field assigned to `gateway-announcements` on the Media-Gateway screen before the Gateway embedded VAL (v VAL) can be enabled. Then the 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 Gateway embedded VAL also can be disabled using the **disable announcement-board ggV9** command. This removes that gateway from the VAL circuit pack count but announcements already assigned and recorded/FTPed on that circuit pack remain but will not play.
Administering Announcements (recording, copying, deleting, and so on.)	*Avaya Aura® Communication Manager Feature Description and Implementation*.
Viewing announcement usage measurements (**list measurements announcement** command)	*Avaya Aura® Communication Manager Reports* and *Avaya Aura® Communication Manager Feature Description and Implementation*.

Table continues…

Task	Information source
Troubleshooting announcements	*Avaya Aura® Communication Manager Feature Description and Implementation*.
Troubleshooting VAL hardware	*Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers* for your model.

Chapter 19: Managing Group Communications

Voice Paging Over Loudspeakers setup

Use this procedure to allow users to make voice pages over an external loudspeaker system connected to Communication Manager. If you're using an external paging system instead of an auxiliary trunk circuit pack, don't use this procedure. External systems typically connect to a trunk or station port and are not administered through the Loudspeaker Paging screen.

For more information about voice paging over loudspeakers, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

See Speakerphone paging setup for another way to let users page.

Preparing to set up Voice Paging Over Loudspeakers

Procedure

Verify that your server running Communication Manager has one or more auxiliary trunk circuit packs with enough available ports to support the number of paging zones you define.

Each paging zone requires 1 port. For information on specific circuit packs, see the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Setting Up Voice Paging Over Loudspeakers example

About this task

As an example, we will set up voice paging for an office with 5 zones. We'll allow users to page all 5 zones at once, and we'll assign a class of restriction of 1 to all zones.

Procedure

1. Enter `change paging loudspeaker`.
2. In the **Voice Paging Timeout** field, enter `30`.

   This field sets the maximum number of seconds a page can last. In our example, the paging party will be disconnected after 30 seconds.
3. In the **Port** field for **Zone 1**, enter `01C0501`.

   Use this field to assign a port on an auxiliary trunk circuit pack to this zone.

4. In the **Voice Paging — TAC** field enter `301`.

   Use this field to assign the trunk access code users dial to page this zone. You cannot assign the same trunk access code to more than one zone.

5. In the **Voice Paging — COR** field enter `1`.

   Use this field to assign a class of restriction to this zone. You can assign different classes of restriction to different zones.

6. On the **Zone 1** row, enter `Reception area` in the **Location** field.

   Give each zone a descriptive name so you can easily remember the corresponding physical location.

7. Repeat steps 4 through 6 for zones 2 to 5.

8. In the **ALL** row, enter `310` in the **Voice Paging — TAC** field and `1` in the **Voice Paging — COR** field.

   By completing this row, you allow users to page all zones at once. You do not have to assign a port to this row.

9. Select `Enter` to save your changes.

   You can integrate loudspeaker voice paging and call parking. This is called “deluxe paging.” You enable deluxe paging by entering `y` in the **Deluxe Paging and Call Park Timeout to Originator** field on the Feature-Related System Parameters screen. To allow paged users the full benefit of deluxe paging, you should also enter a code in the **Answer Back Access Code** field on the Feature Access Code (FAC) screen if you haven’t already: paged users will dial this code + an extension to retrieve calls parked by deluxe paging.

Loudspeaker Paging troubleshooting

This section lists the known or common problems that users might experience with the Loudspeaker Paging feature.

Problem	Possible cause	Action
Users cannot page.	The attendant has control of the trunk group.	Deactivate attendant control.
Calls to an extension are heard over the loudspeakers.	The extension might have been forwarded to a trunk access code used for paging.	Deactivate call forwarding or change the extension to which calls are forwarded.

User considerations for Voice Paging Over Loudspeakers

Users page by dialing the trunk access code assigned to a zone and speaking into their handset. For your users’ convenience, you might also want to consider the following options:

- Add the paging trunk access codes to an abbreviated dialing list and allow users to page using the list.
- Assign individual trunk access codes to Autodial buttons.

- Assign individual trunk access codes to Busy buttons. The status lamp tells the user whether or not the trunk is busy.
- For attendants, you can provide one-button paging access by assigning trunk access codes for paging zones to the Direct Trunk Group Select buttons on the attendant console.

With an appropriate class of restriction, remote callers can also make loudspeaker pages.

When deluxe paging is enabled, if a user with an active call dials the trunk access code for a paging zone the active call is automatically parked.

- Users dial the trunk access code + “#” to page and park an active call on their own extensions.
- Users with console permission can park a call on any extension by dialing the trunk access code + the extension.
- Attendants or users with console permissions can park calls to common shared extensions.
- Parked calls can be retrieved from any telephone. Paged users simply dial the answer back feature access code + the extension where the call is parked.

Chime Paging Over Loudspeakers setup

Use this procedure to allow users to make chime pages over an external loudspeaker system connected to your Avaya Server. Users page by dialing a trunk access code and the extension of the person they want to page. The system plays a unique series of chimes assigned to that extension. This feature is also known as Code Calling Access.

To set up chime paging, you fill out the necessary fields on the Loudspeaker Paging screen and then assign chime codes to individual extensions on the Code Calling IDs screen.

For more information about chime paging over loudspeakers, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

See Speakerphone paging setup below for another way to let users page.

Preparing to set up Chime Paging Over Loudspeakers

Procedure

Verify that your server running Communication Manager has one or more auxiliary trunk circuit packs with enough available ports to support the number of paging zones you define.

Each paging zone requires 1 port. For information on specific circuit packs, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Setting up Chime Paging Over Loudspeakers example

About this task

As an example, we will set up chime paging for a clothing store with 3 zones. We'll allow users to page all zones at once, and we will assign a class of restriction of 1 to all zones.

Procedure

1. Enter `change paging loudspeaker`.
2. In the **Code Calling Playing Cycles** field, enter `2`.

   This field sets the number of times a chime code plays when someone places a page.
3. In the **Port** field for **Zone 1**, enter `01A0301`.

   Use this field to assign a port on an auxiliary trunk circuit pack to this zone.
4. In the **Code Calling — TAC** field enter `80`.

   Use this field to assign the trunk access code users dial to page this zone. You cannot assign the same trunk access code to more than one zone.
5. In the **Code Calling — COR** field enter`1`.

   Use this field to assign a class of restriction to this zone. You can assign different classes of restriction to different zones.
6. On the **Zone 1** row, enter `Men's Department` in the **Location** field.

   Give each zone a descriptive name so you can easily remember the corresponding physical location.
7. Repeat steps 4 through 6 for zones 2 and 3.
8. In the **ALL** row, enter`89` in the **Code Calling — TAC** field and `1` in the **Code Calling — COR** field.

   By completing this row, you allow users to page all zones at once. You do not have to assign a port to this row.
9. Select `Enter` to save your changes.

Assigning chime codes example

Procedure

1. Enter **`change paging code-calling-ids`**.
2. Enter the first extension, `2130`, in the **Ext** field for Id 111.

   Each code Id defines a unique series of chimes.
3. Assign chime codes to the remaining extensions by typing an extension number on the line following each code Id.

   You can assign chime codes to as many as 125 extensions.

4. Select `Enter` to save your changes.

Chime Paging Over Loudspeakers troubleshooting

Problem	Possible causes	Solutions
Users report that they can't page.	The attendant has taken control of the trunk group.	Deactivate attendant control.

User considerations for Chime Paging Over Loudspeakers

Users page by dialing the trunk access code assigned to a zone. For your users' convenience, you might also want to consider the following options:

- Add the paging trunk access codes to an abbreviated dialing list and allow users to page using the list.

  Note:

  Don't use special characters in abbreviated dialing lists used with chime paging.

- Assign individual trunk access codes to Autodial buttons.
- Assign individual trunk access codes to Busy buttons. The status lamp tells the user whether or not the trunk is busy.
- For attendants, you can provide one-button paging access by assigning trunk access codes for paging zones to the **Direct Trunk Group Select** buttons on the attendant console.

With an appropriate class of restriction, remote callers can also make loudspeaker pages.

Speakerphone paging setup

Use this procedure to allow users to make an announcement over a group of digital speakerphones. By dialing a single extension that identifies a group, users can page over all the speakerphones in that group. Speakerphone paging is one-way communication: group members hear the person placing the page but cannot respond directly.

See Group Paging in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information on paging over speakerphones.

Preparing to set up speakerphone paging

Procedure

Verify that you have DCP set speakerphones or IP set speakerphones.

Setting up speakerphone paging example

About this task

To set up speakerphone paging, you create a paging group and assign telephones to it. In the following example, we'll create paging group 1 and add 4 members.

Procedure

1. Type **add group-page 1**.
2. In the **Group Extension** field, enter 3210.

   This field assigns the extension users dial to page the members of this group.
3. In the **Group Name** field, enter `Sales staff`.

   This system displays this name on callers' telephone display when they page the group.
4. In the **COR** field, enter `5`.

   Any user who wants to page this group must have permission to call COR 5.
5. In the `Ext` field in row 1, enter `2009`.
6. Enter the remaining extensions that are members of this group.

   Communication Manager fills in the **Name** fields with the names from the Station screen when you save your changes.
7. Set the **Alert** field to y for telephones that require an alert message to enable ringing, for example, Spectralink wireless telephones.
8. Select `Enter` to save your changes.

Speakerphone paging troubleshooting

Problem	Possible causes	Solutions
Users get a busy signal when they try to page.	All telephones in the group are busy or off-hook.	Wait a few minutes and try again.
	All telephones in the group have Send All Calls or Do Not Disturb activated.	Group members must deactivate these features 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 to hear a page.

Speakerphone paging capacities

- You can create up to 32 paging groups on Communication Manager.
- Each group can have up to 32 extensions in it.

- One telephone can be a member of several paging groups.

Whisper Paging users who are on active calls

Use this procedure to allow one user to interrupt another user's call and make a private announcement. This is called whisper paging. The paging user dials a feature access code or presses a feature button, then dials the extension they want to call. All 3 users can hear the tone that signals the page, but only the person on the paged extension can hear the pager's voice: other parties on the call cannot hear it, and the person making the page cannot hear anyone on the call.

See Whisper Paging in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information on whisper paging.

Preparing to set up Whisper Paging

Procedure

1. Verify that your Communication Manager server has a circuit pack that supports whisper paging.

   For information on specific models, see the *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

2. Verify that your users have 6400-, 7400-, 8400-, or 9400-series DCP (digital) telephones.

Whisper Paging setup

You give users the ability to use whisper paging by administering feature buttons or feature access codes.

You can give users feature buttons that make, answer, or block whisper pages. Using the Station screen, you can administer these buttons in any combination as appropriate:

- Whisper Page Activation — to place a whisper page.
- Answerback — 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— 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 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*, for information about the screens referred in this topic.

Telephones as Intercoms administration

Use this feature to make communications quicker and easier for users who frequently call each other. With the intercom feature, you can allow one user to call another user in a predefined group just by pressing a couple of buttons. You can even administer a button that always calls a predefined extension when pressed.

Administering the intercom feature is a 2-step process. First, you create an intercom group and assign extensions to it. Then, to allow group members to make intercom calls to each other, you administer feature buttons on their telephones for automatic intercom, dial intercom, or both. This section also provides instructions for allowing one user to pick up another user's intercom calls.

See Abbreviated Dialing in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for information on another way for users to call each other without dialing complete extension numbers.

See Intercom in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for detailed information on intercom functions.

Administering intercom feature buttons example

About this task

To allow users to make intercom calls, you must administer feature buttons on the telephones in the intercom group. You can administer buttons for dial intercom, automatic intercom, or both on multi-appearance telephones. You can't administer either intercom feature on single-line telephones, but you can assign single-line telephones to intercom groups so those users can receive intercom calls.

As an example, we will set up automatic intercom between extensions 2010 (dial code = 1) and 2011 (dial code = 2) in intercom group 1.

Procedure

1. Enter **`change station 2010`**.
2. Move to the page with the **BUTTON ASSIGNMENTS** fields.
3. In **BUTTON ASSIGNMENTS** field 4, enter `auto-icom`.

   Press `Tab`.

   The **Grp** and **DC** fields appear.
4. In the **Grp** field, enter `1`.

   This is the number of the intercom group. Since an extension can belong to more than one intercom group, you must assign a group number to intercom buttons.
5. In the **DC** field, enter `2`.

   This is the dial code for extension 2011, the destination extension.
6. Select `Enter` to save your changes.

7. Repeat steps 1 to 6 for extension 2011.

   Assign a dial code of 1 to 2011's automatic intercom button.

   To give a member of a group the ability to make intercom calls to all the other members, administer a Dial Intercom button on the member's telephone. Type the number of the intercom group in the **Grp** field beside the **Dial Intercom** button.

   You can also give one user instant, one-way access to another. For example, to give user A instant, one-way access to user B, administer an **Automatic Intercom** button on A's telephone only. You don't have to administer any intercom button on B's telephone. If B has a Dial Intercom button, he can make an intercom call to A the same way as he would to any other group member.

   When users are in the same call pickup group, or if Directed Call Pickup is enabled on your server running Communication Manager, one user can answer an intercom call to another user. To allow users to pick up intercom calls to other users, you must enter `y` in the **Call Pickup on Intercom Calls** field on the Feature-Related System Parameters screen.

Administering an intercom group example

About this task

In this example, we'll create intercom group 1 and add extensions 2010 to 2014

Procedure

1. Enter `add intercom-group 1`
2. Enter `1` in the **Length of Dial Code** field.

   Dial codes can be 1 or 2 digits long.
3. On row 1, enter `2010` in the **Ext** field.
4. On row 1, enter `1` in the **DC** field.

   This is the code a user will dial to make an intercom call to extension 2010. The length of this code must exactly match the entry in the **Length of Dial Code** field.
5. Repeat steps 3 and 4 for the remaining extensions.

   Dial codes don't have to be in order. Communication Manager fills in the **Name** field with the name from the Station screen when you save changes.
6. Select `Enter` to save your changes.

Automatic Answer Intercom Calls setup

About this task

A user can use Automatic Answer Intercom Calls (Auto Answer ICOM) to answer an intercom call within the intercom group without pressing the intercom button. Auto Answer ICOM works with digital, BRI, and hybrid telephones with built-in speaker, headphones, or adjunct speakerphone.

Security alert:

Press the **Do Not Disturb** button or the **Send All Calls** button on your telephone when you don't want someone in your intercom group to listen in on a call. Auto Answer ICOM does not work when the **Do Not Disturb** button or the **Send All Calls** button is pressed on the telephone.

Administering Auto Answer ICOM example

About this task

This section contains an example, with step-by-step instructions, on how to set up Auto Answer ICOM.

In this example, you set up Auto Answer ICOM on station 12345.

Procedure

1. Enter `change station 12345`.

   The system displays the Station screen for extension 12345. Click **Next Page** until you see the Feature Options page.

2. Move to the **Auto Answer** field and enter `icom`.
3. Select `Enter` to save your changes.

Service Observing Calls

About this task

Use this procedure to allow designated users, normally supervisors, to listen to other users' calls. This capability is often used to monitor service quality in call centers and other environments where employees serve customers over the telephone. On Communication Manager, this is called "service observing" and the user observing calls is the "observer."

This section describes service observing in environments without Automatic Call Distribution (ACD) or call vectoring. To use service observing in those environments, see *Avaya Aura® Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568.

See Service Observing in *Avaya Aura® Communication Manager Feature Description and Implementation*, 55-245-205, for detailed information on service observing.

Preparing to set up Service Observing

1. On the System Parameter Customer-Options screen, verify that the:
   - **Service Observing (Basic)** field is y.
2. If you want to enable remote service observing by allowing remote users to dial a feature access code, verify the:
   - **Service Observing (Remote/By FAC)** field is y.

If the appropriate field is disabled, go to the Avaya Support website at http://support.avaya.com.

Setting up Service Observing example

About this task

Security alert:

Listening to someone else's calls might be subject to federal, state, or local laws, rules, or regulations. It might require the consent of one or both of the parties on the call. Familiarize yourself with all applicable laws, rules, and regulations and comply with them when you use this feature.

In this example, we'll set up service observing for a manager. The manager's class of restriction is 5. We'll assign a feature button to the manager's telephone and allow her to monitor calls on local extensions that have a class of restriction of 10. Everyone on an observed call will hear a repetitive warning tone.

Procedure

1. Set the observer's class of restriction to permit service observing:
   a. In the Class of Restriction screen for COR 5, enter y in the **Can Be A Service Observer** field.
   b. Move to the page of the Class of Restriction screen that shows service observing permissions.
   c. Enter y in the field for class of restriction 10.
2. In the Class of Restriction screen for COR 10, enter y in the **Can Be Service Observed** field.

   Anyone with class of restriction 5 now has permission to observe extensions with class of restriction 10. To further restrict who can observe calls or be observed, you might want to create special classes of restriction for both groups and use these classes only for the appropriate extensions.
3. In the Station screen, assign a **Service Observing** button to the observer's telephone.

   A service observing button permits users to switch between listen-only and listen-and-talk modes simply by pressing the button.
4. To activate the warning tone, enter y in the **Service Observing — Warning Tone** field on the Feature-Related System Parameters screen.

A unique 2-second, 440-Hz warning tone plays before an observer connects to the call. While the call is observed, a shorter version of this tone repeats every 12 seconds.

5. For users to activate service observing by feature access codes, use the Feature Access Code (FAC) screen to administer codes in one or both of the following fields:
   - **Service Observing Listen Only Access Code**
   - **Service Observing Listen/Talk Access Code**

   When using feature access codes, observers must choose a mode at the start of the session. They cannot switch to the other mode without ending the session and beginning another.

Note:

Feature access codes are required for remote observing.

Best practices for service observing

Procedure

1. Do not add a bridged appearance as line appearance 1 for any station.

   Doing this can cause unexpected feature interactions with features like Service Observing and TTI.

2. You can observe calls on a primary extension as well as all bridged appearances of that extension.

   You cannot observe the bridged appearances on the bridged extension's telephone. For example, if you are observing extension 3082 and this telephone also has a bridged appearance for extension 3282, you cannot observe calls on the bridged call appearance for 3282. But if you observe extension 3282, you can observe activity on the primary and all of the bridged call appearances of 3282.

3. If you are a primary telephone user or a bridging user, you can bridge onto a service observed call of the primary at any time.

   If you are a bridging user, you cannot activate Service Observing using a bridged call appearance.

4. If the primary line is service observing on an active call, a bridged call appearance cannot bridge onto the primary line that is doing the service observing.

Chapter 20: Managing Data Calls

Types of Data Connections

You can use Communication Manager to allow the following types of data elements or devices to communicate to the world:

- Data Terminals
- Personal Computers
- Host Computers (for example, CentreVu CMS)
- Digital Telephones (Digital Communications Protocol (DCP) and Integrated Services Digital Network-Basic Rate Interface (ISDN-BRI))
- Audio or 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 or modem pooling circuit packs

Once you have connected these data devices to Communication Manager, you can use networking and routing capabilities to allow them to communicate with other devices over your private network or the public network.

This section describes the system features available to enable data communications.

Data Call Setup

Data Call Setup provides multiple methods to set up a data call:

- Data-terminal (keyboard) dialing

- Telephone dialing
- Hayes AT command dialing
- Administered connections
- Hotline dialing

Data Call Setup Administration

Administering Data Call Setup for data-terminal dialing

Procedure

1. Choose one of the following data modules and administer all fields:
   - Processor or Trunk Data Module
   - Data Line Data Module
   - 7500 Data Module
2. On the Modem Pool Group screen, administer the **Circuit Pack Assignments** field.

Administering Data Call Setup for telephone dialing

Procedure

1. Choose one of the following:
   - On the Feature Access Code (FAC) screen, administer the **Data Origination Access Code** field. For more information about this field, see *Avaya Aura® Communication Manager Screen Reference*.
   - On the Station screen, assign one button as data-ext (Ext:).
2. Choose one of the following data modules and administer all fields:
   - Processor or Trunk Data Module
   - Data Line Data Module
3. On the Modem Pool Group screen, administer the **Circuit Pack Assignments** field.

Data Call Setup port assignments

Depending on the hardware used, assign ports to the following:

- Data modules
- 7400D-series or CALLMASTER digital telephones
- 7500D-series telephones with asynchronous data module (ADM)
- Analog modems (port is assigned using 2500 telephone screen)

Characters used in Data Call Setup

Basic-digit dialing is provided through an ADM or 7500B data module. The user can enter digits from 0 to 9, *, and # from a 7500 or 8500 series telephone keypad or an EIA-terminal interface. In addition, the user can dial the following special characters.

Table 2: Special characters

Character	Use
SPACE, -, (, and)	improves legibility. Communication Manager ignores these characters during dialing.
+ character (wait)	interrupts or suspends dialing until the user receives dial tone
, (pause)	inserts a 1.5-second pause
% (mark)	indicates digits for end-to-end signaling (touch-tone). This is required when the trunk is rotary. It is not required when the trunk is touch-tone.
UNDERLINE or **BACKSPACE**	corrects previously typed characters on the same line
@	deletes the entire line and starts over with a new DIAL: prompt

Each line of dialing information can contain up to 42 characters (the + and % characters count as two each).

Examples of dialing are:

- DIAL: 3478
- DIAL: 9+(201) 555-1212
- DIAL: 8, 555-2368
- DIAL: 9+555-2368+%9999+123 (remote access)

DCP and ISDN-BRI module call-progress messages

The following call-progress messages and their meanings are provided for DCP and ISDN-BRI modules.

Table 3: Call-progress messages

Message	Application	Meaning
DIAL:	DCP	Equivalent to dial tone. Enter the required number or FAC followed by Enter.
CMD	BRI	Equivalent to dial tone. Enter the required 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.

Table continues…

Message	Application	Meaning
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 unavailable.
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.
INVALID ADDRESS	DCP	Entered name is not in alphanumeric-dialing table.
WRONG ADDRESS	BRI	Entered name is not in alphanumeric-dialing table.
PLEASE ANS-	DCP, BRI	Originating telephone user transferred call to data module using One-Button Transfer to Data.
TRANSFER	DCP	Data Call Return-to-Voice is occurring.
CONFIRMED	DCP, BRI	Equivalent to confirmation tone. Feature request is accepted, or call has gone to a local coverage point.
OTHER END	DCP, BRI	Endpoint has terminated call.
DISCONNECTED	DCP, BRI	Call is disconnected.
WAIT	DCP, BRI	Normal processing continues.
WAIT, XX IN QUEUE	DCP	Call is in a local hunt-group queue.

DCP data modules

Using DCP data-terminal dialing

About this task

A user can use DCP data-terminal dialing to set up and disconnect data calls directly from a data terminal as follows.

Procedure

1. At the **DIAL** prompt, the user types the data number.
2. If the call is queued, the message **WAIT, XX IN QUEUE** displays.

   The queue position XX updates as the call moves up in queue.

3. To originate and disconnect a call, the user presses **BREAK**.

   If the terminal does not generate a two-second continuous break signal, the user can press originate or disconnect on the data module.

4. The user can enter digits at the **DIAL**: prompt.

DCP telephone dialing

Telephone users can use DCP telephone dialing to originate and control data calls from a telephone.

Users can set up a call using any unrestricted telephone and then transfer the call to a data endpoint.

The primary way to make data calls is with multiappearance telephone data-extension buttons. Assign any administrable feature button as a data-extension button. The data-extension button provides one-touch access to a data module. The number of assigned data-extension buttons per telephone is not limited.

The following options, either alone or combined, permit flexibility in making data calls from a telephone.

- One-Button Transfer to Data

  A user can transfer a call to the associated data module by pressing the data-extension button after the endpoint answers.

- Return-to-Voice

  A user can change the connection from data to voice. The user presses the data-extension button associated with the busy data module. If the user hangs up, the call disconnects. Return of a data call to the telephone implies that the same data call is continued in the voice mode, or transferred to point.

  The Return-to-Voice feature is denied for analog adjuncts.

- Data Call Preindication

  A user, before dialing a data endpoint, can reserve the associated data module by pressing the data-extension button. This ensures that a conversion resource, if needed, and the data module are reserved for the call. Avaya recommends the use of Data Call Preindication before 1-button transfer to data for data calls that use toll-network facilities. Data Call Preindication is in effect until the associated data-extension button is pressed again for a 1-button transfer; there is no time-out.

ISDN-BRI data modules

Using ISDN-BRI data-terminal dialing

About this task

Your can set up and disconnect data calls directly from a data terminal without using a telephone as follows:

Procedure

1. Press `Enter` a few times.
2. If the CMD: prompt does not appear, press **Break A + T** at the same time, and then press `Enter`..
3. At the **CMD**: prompt, the user types and presses au `Enter`.
4. To disconnect, enter +++.
5. At the CMD: prompt, the type end and press `Enter`.

ISDN-BRI telephone dialing

To make a data call, an ISDN-BRI telephone user presses the data button on the terminal, enters the number on the dial pad, and then presses the data button again.

The following data functions are unavailable on ISDN-BRI telephones:

- One-Button Transfer to Data
- Return-to-Voice
- Data Call Preindication
- Voice-Call Transfer to Data and Data-Call Transfer to Voice

The system handles all presently defined BRI bearer data-call requests. Some capabilities that are not supported by Avaya terminals are provided by non-Avaya terminals. If Communication Manager does not support a capability, a proper cause value returns to the terminal.

BRI terminals receive a cause or reason code that identifies why a call is being cleared. The BRI data module converts certain cause values to text messages for display.

In a passive-bus multipoint configuration, the system supports two BRI endpoints per port, thus doubling the capacity of the BRI circuit pack. When you change the configuration of a BRI from point-to-point to multipoint, the original endpoint does not need to reinitialize. Only endpoints that support service profile identifier (SPID) initialization can be administered in a multipoint configuration.

Analog modems

When a telephone user places a data call with a modem, the user dials the data-origination access code assigned in the system before dialing the endpoint.

Considerations for Data Call Setup

- A BRI telephone cannot call a data terminal, and a data terminal cannot call a BRI telephone.

Interactions for Data Call Setup

- Abbreviated Dialing

Only 22 of the 24 (maximum) digits in an abbreviated-dialing number are available for keyboard dialing. The remaining two digits must contain the wait indicator for tone detection.

- Call Coverage

  A hunt group made up of data endpoints cannot be assigned a coverage path.

- Call Detail Recording

  CDR records the use of modem pools on trunk calls.

- Call Forwarding All Calls

  Calls received by a data module can be forwarded. Activate Call Forwarding All Calls with data-terminal (keyboard) dialing. If the forwarded-to endpoint is an analog endpoint and the caller is a digital endpoint, modem pooling is activated automatically.

- Pooled Modems with Hunt Groups

  UCD can provide a group of data modules or analog modems for answering calls to connected facilities (for example, computer ports).

- World-Class Tone Detection

  Multiple-line data-terminal dialing is supported if the administered level of tone detection is precise. You can administer tone-detection options. The message that Data Call Setup sends to users varies according to the option.

  If the option is not set to precise, and a data call is set up over an analog trunk, messages describing the status of the called endpoint (for example, RINGING, BUSY, TRY AGAIN) change according to which tone-detection option is selected.

Alphanumeric Dialing

Alphanumeric Dialing enhances data-terminal dialing using which users can 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.

You can use Alphanumeric Dialing to change a mapped string (digit-dialing address) without having to inform all users of a changed dial address. Users dial the alpha name.

When a user enters an alphanumeric name, the system converts the name to a sequence of digits according to an alphanumeric-dialing table. If the entered name is not found in the table, the system denies the call attempt and the user receives either an `Invalid Address` message (DCP) or a `Wrong Address` message (ISDN-BRI).

Because data terminals access Communication Manager via DCP or ISDN-BRI data modules, dialing procedures vary:

- For DCP, at the `DIAL`: prompt users type the alphanumeric name. Press `Enter`.

- For ISDN-BRI, at the `CMD`:prompt users type `d`, a space, and the alphanumeric name. Press `Enter`.

More than one alphanumeric name can see the same digit string.

Administering Alphanumeric Dialing

Procedure

On the Alphanumeric Dialing Table screen, administer the **Alpha-name** and **Mapped String** fields.

Considerations for Alphanumeric Dialing

Note:

Alphanumeric dialing does not apply to endpoints with Hayes modems.

Data Hotline

Data Hotline provides for automatic-nondial placement of a data call preassigned to an endpoint when the originating server goes off-hook. Use for security purposes.

The endpoint can be used for hotline dialing if the users can use the endpoint software to select the dial function without entering a number.

Administering Data Hotline

About this task

You can use an abbreviated dialing list for your default ID. See Abbreviated Dialing in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for more information.

Procedure

1. On the Station screen, administer the following fields.
   - **Abbreviated Dialing List**
   - **Special Dialing Option**
   - **Hot Line Destination**
2. On the Data Module screen, administer the **Abbreviated Dialing List1** field.

   The system automatically places Data Hotline calls to preassigned extensions or off-premises numbers. Calling terminals are connected to the system by a data module. Users should store the destination number in the abbreviated dialing list for future reference.

Interactions for Data Hotline

- Call Forwarding — All Calls

  A Data Hotline caller cannot activate both Call Forwarding and Data Hotline. Dialing the Call Forwarding feature access code (FAC) causes activation of the Data Hotline instead.

Data Privacy

Data Privacy protects analog data calls from being disturbed by any of the system's overriding or ringing features.

Administering Data Privacy

Procedure

1. On the Feature Access Code (FAC) screen, administer the **Data Privacy Access Code** field.
2. On the Class of Service screen, administer the **Data Privacy** field.
3. On the Station screen, administer the **Class of Service** field.

   To activate this feature for a call, the user must dial the Data Privacy FAC in the beginning of the call. If Data Privacy is disabled on the calling station's COS, the user hears intercept tone immediately after dialing the Data Privacy FAC.

Considerations for Data Privacy

- Data Privacy applies to both voice and data calls. You can activate Data Privacy on Remote Access calls, but not on other incoming trunk calls. Data Privacy is canceled if a user transfers a call, is added to a conference call, is bridged onto a call, or disconnects from a call. You can activate Data Privacy on calls originated from attendant consoles.
- For virtual extensions, assign the Data Privacy Class of Service to the mapped-to physical extension.

Interactions for Data Privacy

- Attendant Call Waiting and Call Waiting Termination

  If Data Privacy is active, Call Waiting is denied.

- Bridged Call Appearance — Single-Line Telephone

  If you activate Data Privacy or assign Data Restriction to a station involved in a bridged call and the primary terminal or bridging user attempts to bridge onto the call, this action overrides Data Privacy and Data Restriction.

- Busy Verification

Busy Verification cannot be active when Data Privacy is active.

- Intercom — Automatic and Dial

  An extension with Data Privacy or Data Restriction active cannot originate an intercom call. The user receives an intercept tone.

- Music-on-Hold Access

  If a user places a call with Data Privacy on hold, the user must withhold Music-on-Hold to prevent the transmission of tones that a connected data service might falsely interpret as a data transmission.

- Priority Calls

  If a user activates Data Privacy, Priority Calls are denied on analog telephones. However, Priority Calls appear on the next available line appearance on multiappearance telephones.

Default Dialing

Default Dialing provides data-terminal users who dial a specific number the majority of the time a very simple method of dialing that number. Normal data terminal dialing and alphanumeric dialing are unaffected.

Default Dialing enhances data terminal (keyboard) dialing using which a data terminal user can place a data call to a pre-administered destination by either pressing `Enter` at the DIAL: prompt (for data terminals using DCP data modules) or typing `d` and pressing `Enter` at the CMD: prompt (for data terminals using ISDN-BRI data modules). The data-terminal user with a DCP data module can place calls to other destinations by entering the complete address after the DIAL: prompt (normal data terminal dialing or alphanumeric dialing). The data-terminal user with an ISDN-BRI data module can place calls to other destinations by typing `d`, a space, the complete address. Press `Enter` after the CMD: prompt.

Note:

DU-type hunt groups connecting the system to a terminal server on a host computer have hunt-group extensions set to `no` keyboard dialing.

For the AT command interface supported by the 7400A/7400B/8400B data module, to dial the default destination, enter the ATD command (rather than press return).

Administering Default Dialing

About this task

You can use an abbreviated dialing list for your default ID. See Abbreviated Dialing in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205, for more information.

Procedure

On the Data Module screen, administer the following fields:

- **Special Dialing Option** as default.
- **Abbreviated Dialing List**, enter the list to use.
- **AD Dial Code**.

Data Restriction

Data Restriction protects analog-data calls from being disturbed by any of the system's overriding or ringing features or system-generated tones.

Data Restriction applies to both voice and data calls.

Once you administer Data Restriction for an analog or multiappearance telephone or trunk group, the feature is active on all calls to or from the terminal or trunk group.

Note:

Do not assign Data Restriction to attendant consoles.

Administering Data Restriction

Procedure

1. On the Station screen, set the **Data Restriction** field to `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 for Data Restriction

- Attendant Call Waiting and Call Waiting Termination

  If Data Restriction is active, Call Waiting is denied.

- Busy Verification

  Busy Verification cannot be active when Data Restriction is active.

- Intercom — Automatic and Dial

  An extension with Data Privacy or Data Restriction activated cannot originate an intercom call. The user receives an Intercept tone.

- Music-on-Hold Access

  If a user places a call with Data Restriction on hold, The user must withhold Music-on-Hold to prevent the transmission of tones that a connected data service might falsely interpret as a data transmission.

- Priority Calls

  Priority Calls are allowed if the analog station is idle. Call Waiting (including Priority Call Waiting) is denied if the station is busy. However, Priority Calls appear on the next available line appearance on multiappearance telephones.

- Service Observing

  A data-restricted call cannot be service observed.

Data-Only Off-Premises Extensions

Users can use Data-Only Off-Premises Extensions to make data calls involving data communications equipment (DCE) or digital terminal equipment (DTE) located remotely from the system site.

A Data-Only Off-Premises Extension uses an on-premises modular trunk data module (MTDM). The system communicates with remote data equipment through the private-line facility linking the on-premises MTDM and the remote data equipment.

Users can place data calls to this type of data endpoint using Telephone Dialing or Data Terminal (Keyboard) Dialing. Since there is no telephone at the remote site, originate data calls from the remote data terminal using Keyboard Dialing only.

Administering Data-Only Off-Premises Extensions

Procedure

On the Processor/Trunk Data Module screen, administer all fields.

For more information, see Data Module in *Avaya Aura® Communication Manager Screen Reference*, for more information.

Considerations for Data-Only Off-Premises Extensions

The system does not support communications between two TDMs. Modem Pooling is similar to a TDM, it cannot be used on calls to or from a Data-Only Off-Premises Extension.

Interactions for Data-Only Off-Premises Extensions

- Telephone Dialing

  An on-premises multiappearance telephone might have a Data Extension button associated with the TDM used for a Data-Only Off-Premises Extension. The telephone user and the remote user share control of the data module. Actions of the user at the telephone might affect the remote user.

  - 1-Button Transfer to Data

    The telephone user can transfer a call to the Data-Only Off-Premises Extension. The Data Extension button lamp on the telephone lights and the Call in Progress lamp on the data module lights during a data call.

  - Data Call Preindication

    The multiappearance telephone user presses the idle associated Data Extension button to reserve a data module. The data module is busy to all other users. When the user reserves a data module, the lamp associated with the Data Extension button winks and lights at any other associated telephones. A remote user receives the BUSY message when attempting to originate a call.

  - Return-to-Voice

    To establish a data call, the telephone user presses the associated busy Data Extension button to transfer the call to the telephone. The data module associated with the Data Extension button is disconnected from the call. The Call in Progress lamp on the data module goes dark.

Data Modules — General

A data module is a connection device between a basic-rate interface (BRI) or DCP interface of the Avaya 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 or 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 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 Personal Computer communications packages.

Administered Connections

Use the Administered Connections (AC) feature to establish an end-to-end connection between two access or data endpoints. Communication Manager automatically establishes the connection based on the attributes that you administer. The Administered Connections feature provides the following abilities:

- Support of both permanent and scheduled connections
- Autorestoration (preserving the active session) for connections that are routed over Software Defined Data Network (SDDN) trunks
- An administrable retry interval from 1 to 60 minutes for each AC
- An administrable alarm strategy for each AC
- An establish, retry, autorestoration order that is based on administered priority

Detailed description of Administered Connections

Establish an AC between the following:

- Two endpoints on the same Avaya DEFINITY® server or Avaya Server
- Two endpoints in the same private network, but on different servers
- One endpoint on the controlling server and another endpoint off the private network

In all configurations, administer the AC on the server having the originating endpoint. For an AC in a private network, if the two endpoints are on two different servers, normally the connection routes via Automatic Alternate Routing (AAR) through tie trunks (ISDN, DS1, or analog tie trunks) and intermediate servers. If required, route the connection via Automatic Route Selection (ARS) and Generalized Route Selection (GRS) through the public network. The call routes over associated ISDN trunks. When the far-end answers, a connection occurs between the far-end and the near-end extension in the `Originator` field on the Administered Connection screen.

Because the system makes an administered connection automatically, you do not use the following:

- Data Call Setup

  Do not assign a default dialing destination to a data module when it is used in an AC.

- Data Hotline

  Do not assign a hotline destination to a data module that is used in an AC.

- Terminal Dialing

  Turn off terminal dialing for data modules involved in an AC. This prevents display of call-processing messages (INCOMING CALL) on the terminal.

Access endpoints used for Administered Connections

Access endpoints are nonsignaling trunk ports. Access endpoints neither generate signaling to the far-end of the trunk nor respond to signaling from the far-end. You designate an access endpoint as the originating endpoint or the destination endpoint in an AC.

Typical applications for Administered Connections

The following examples are typical AC applications:

- A local data endpoint that connects to a local or a remote access endpoint, such as:
  - A modular processor data model (MPDM) ACCUNET digital service that connects to SDDN over an ISDN trunk-group DS1 port; an MPDM
  - An MPDM ACCUNET digital service that connects to an ACCUNET Switched 56 Service over a DS1 port
- A local-access endpoint that connects to a local or a remote access endpoint, such as a DSO cross-connect and a 4-wire leased-line modem to a 4-wire modem connection over an analog tie trunk
- A local data endpoint that connects to a local or a remote data endpoint such as a connection between two 3270 data modules

Conditions for establishing Administered Connections

The originating server attempts to establish an AC only if one of the following conditions exist:

- AC is active.
- AC is due to be active. That is, the AC is a permanent AC, or it is the administered time-of-day for a scheduled AC.
- The originating endpoint is in the in-service or idle state.

If the originating endpoint is not in service or is idle, no activity takes place for the AC until the endpoint transitions to the necessary state. The originating server uses the destination address to route the call to the required endpoint. When the server establishes two or more ACs at the same time, the server arranges the connections in order of priority.

AC attempts can fail because:

- Resources are unavailable to route to the destination.
- A required conversion resource is unavailable.

- Access is denied by Class of Restriction (COR), facilities restriction level (FRL), Bearer Capability Class (BCC), or an attempt is made to route voice-band data over SDDN trunks in the public switched network.
- The destination address is incorrect.
- The destination endpoint is busy.
- Other network or signaling failures occur.

In the event of a failure, an error is entered into the error log. This error generates an alarm, if your alarming strategy warrants an alarm. You can display AC failures with the **`display status-administered connection`** command. The originating server continues to try to establish an AC as long as an AC is scheduled to be active, unless the attempt fails because of an administrative error (for example, a wrong number) or a service-blocking condition, such as outgoing calls are barred).

- The administered retry interval of 1 to 60 minutes for each AC determines the frequency with which failed attempts are retried.
- Retries are made after the retry interval elapses, regardless of the restorable attribute of the AC.
- ACs are retried in priority order.
- When you change the time of day on the server, an attempt is made to establish all ACs in the waiting-for-retry state.

Conditions for dropping Administered Connections

An AC remains active until one of the following scenarios occurs:

- The AC is changed, disabled, or removed.
- The time-of-day requirements of a scheduled AC are no longer satisfied.
- One of the endpoints drops the connection. An endpoint might drop a connection because of user action (in the case of a data endpoint), maintenance activity that results from an endpoint failure, busying out of the endpoint, or handshake failure. If the endpoints are incompatible, the connection is successful until handshake failure occurs.

  Note:

  An AC between access endpoints remains connected even if the attached access equipment fails to handshake.

- An interruption, such as a facility failure, occurs between the endpoints. If an AC drops because the AC was disabled, removed, or is no longer due to be active, no action is taken. If an AC drops because of changed AC attributes, the system makes an immediate attempt to establish the connection with the changed attributes, if the AC is still scheduled to be active. Existing entries in the error or alarm log are resolved if the entries no longer apply. If an AC involves at least one data endpoint, and handshake failure causes the connection

to be dropped, no action is taken for that AC until you run the **`change administered-connection`** command.

Autorestoration and fast retry

When an active AC drops prematurely, you must invoke either autorestoration or fast retry for autorestoration to be attempted for an active AC. If you administer an AC for autorestoration and the connection was routed over SDDN trunks, auto restoration is attempted. During restoration, connections are maintained between the server and both endpoints. In addition to maintaining the active session, AC also provides a high level of security by prohibiting other connections from intervening in active sessions. Autorestoration is usually complete before the 60-second endpoint holdover interval. If autorestoration is successful, the call might be maintained, but this is not guaranteed. The restoration is transparent to the user, with the exception of a temporary disruption of service while restoration is in progress. A successful restoration is indicated by the restored value in the **Connection State** field on the Administered-Connection Status screen. Although a restoration is successful, the data session might not be preserved.

If autorestoration is inactive, or if the AC is not routed over SDDN trunks, the server immediately attempts a fast retry to reestablish the connection. The server also attempts a retry if the originating endpoint caused the drop. With fast retry, connections are not maintained on both ends. Fast retry is not attempted for an AC that was last established with fast retry, unless that AC is active for at least 2 minutes. If autorestoration or fast retry fails to restore or reestablish the connection, the call drops, and the AC goes into retry mode. Retry attempts continue, at the administered retry interval, as long as the AC is scheduled to be active.

Administering Administered Connections

Procedure

1. Choose one of the following data modules and administer all fields:
   - Data Line Data Module (use with Data Line circuit pack)
   - Processor/Trunk Data Module (use with one of the following:)
     - MPDMs, 700D, 7400B, 7400D, or 8400B
     - MTDMs, 700B, 700C, 700E, or 7400A
   - Processor Interface Data Module (for more information, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504)
   - 25 Data Module (for more information, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504)
   - 7500 Data Module (use with ISDN Line 12-BRI-S-NT or ISDN Line 12-BRI-U-NT circuit pack)

- World Class Core BRI Data Module (use with wcbri)

2. On the DS1 Circuit Pack screen, administer all fields.

   Use with switch node carriers.

3. On the Access Endpoint screen, administer all fields.
4. On the Trunk Group screen, choose one of the following trunk groups and administer all fields.
   - ISDN-BRI
   - ISDN-PRI
   - Tie
5. On the Class of Restriction screen, administer all fields.
6. On the Class of Service screen, administer all fields.
7. On the Dial Plan Parameters screen, administer the **Local Node Number** field with a number from 1-63 that matches the DCS switch node number and the CDR node number.
8. On the Administered Connection screen, administer all fields.
9. On the Station screen, assign one button as ac-alarm.
10. On the Attendant Console screen, assign one button as ac-alarm.

Interactions for Administered Connections

- Abbreviated Dialing

  Use Abbreviated Dialing entries in the `Destination` field. Entries must comply with restrictions.

- Busy Verification of Stations and Trunks

  This feature does not apply to access endpoints because they are used only for data.

- Call Detail Recording

  For an AC that uses a trunk when CDR is active, the origination extension is the originator of the call.

- Class of Restriction

  Reserve a COR for AC endpoints and SDDN trunks. This restricts endpoints that are not involved in AC from connecting to SDDN trunks or endpoints involved in AC.

- Class of Service/Call Forwarding

  Assign to an AC endpoint a COS that blocks Call Forwarding activation at the endpoint.

- Digital Multiplexed Interface (DMI)

Use DMI endpoints as the destination in an AC. DMI endpoints do not have associated extensions, so do not use them as the originator in an AC.

- Facility Test Calls

  The feature does not apply to access endpoints because an access endpoint acts as an endpoint rather than as a trunk.

- Modem Pooling

  If you require a modem in an AC, one is inserted automatically. If no modem is available, the connection is dropped.

- Non-Facility Associated Signaling (NFAS) and D-Channel Backup

  Auto restoration for an AC that is initially routed over an NFAS facility can fail if the only backup route is over the facility on which the backup D-channel is administered. The backup D-channel might not come into service in time to handle the restoration attempt.

- **`Set Time`** Command

  When you change the system time via the **`set time`** command, all scheduled ACs are examined. If the time change causes an active AC to be outside its scheduled period, the AC is dropped. If the time change causes an inactive AC to be within its scheduled period, Communication Manager attempts to establish the AC.

  If any AC (scheduled or continuous) is in retry mode and the system time changes, Communication Manager attempts to establish the AC.

- System Measurements

  Access endpoints are not measured. All other trunks in an AC are measured as usual.

Modem Pooling

Modem Pooling allows switched connections between digital-data endpoints (data modules) and analog-data endpoints via pods of acoustic-coupled modems. The analog-data endpoint is either a trunk or a line circuit.

Data transmission between a digital data endpoint and an analog endpoint requires conversion through a modem, because the DCP format used by the data module is incompatible 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 unavailable in countries that use A-law companding.

Combined-conversion modem pools are TDMs cabled to any TDM-compatible modem. Combined-conversion modem pools can be used with all systems.

The system can detect the needs for a modem. Data calls from an analog-data endpoint require that the user indicate the need for a modem, because the system considers such calls to be voice calls. Users indicate this need by dialing the data-origination access code field on the Feature Access Code (FAC) screen before dialing the digital-data endpoint.

The system provides a Hold Time parameter to specify the maximum time any modem can be held but not used (while a data call is in queue).

Administering Integrated Modem Pooling

Procedure

1. On the Modem Pool Group screen, administer all fields.
2. On the Feature Access Code (FAC) screen, administer the **Data Origination Access Code** field.
3. On the Data Module screen, administer all fields.

Administering Combined Modem Poolings

Procedure

1. On the Modem Pool Group screen, administer all fields.
2. On the Feature Access Code (FAC) screen, administer the **Data Origination Access Code** field.

Considerations for Modem Pooling

- On data calls between a data module and an analog-data endpoint, Return-to-Voice releases the modem and returns it to the pool. The telephone user connects to the analog-data endpoint.
- For traffic purposes, the system accumulates data on modem-pooling calls separate from voice calls. Measurements on the pools also accumulate.
- Modem Pooling is unrestricted. 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.

Personal Computer Interface

The personal computer (PC) Interface consists of the Personal Computer/PBX platforms and Personal Computer/ISDN Platform product family. These products are used with Communication Manager to provide users of IBM-compatible Personal Computers fully-integrated voice and data workstation capabilities.

Two groups of different configurations are available for Personal Computer 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 Avaya Server. Group 1 (shown in DCP PC interface configuration (Group 1) on page 409) uses the following connections:

- The Personal Computer Interface card plugs into an expansion slot on the Personal Computer. The card has 2 standard 8-pin modular jacks (line and telephone).
- The digital telephone plugs into the telephone jack on the Personal Computer Interface card.
- The line jack on the card provides a digital port connection to Avaya servers.
- The distance between the Personal Computer Interface card and the PBX should be no more than 1524m for 24-gauge wire or 1219m for 26-gauge wire.

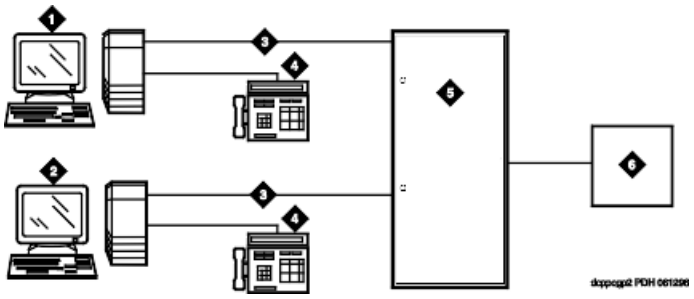


Figure 11: DCP Personal Computer interface configuration (Group 1)

Table 4: Figure notes:

1. IBM-compatible Personal Computer with DCP Interface card
2. IBM-compatible Personal Computer 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 Personal Computer/ISDN Interface card installed in the Personal Computer. This group can include a stand-alone Personal Computer terminal, or up to 4 telephones, handsets, or headsets. Group 2 (shown in the figure on page 410) uses Personal Computer/ISDN Interface cards (up to four cards) which plug into expansion slots on the Personal Computer. These cards each provide 2 standard 8-pin modular-jack connections

for both line connections (to the Avaya Server) and telephone connections. A standard 4-pin modular jack is also available for use with a handset or headset.

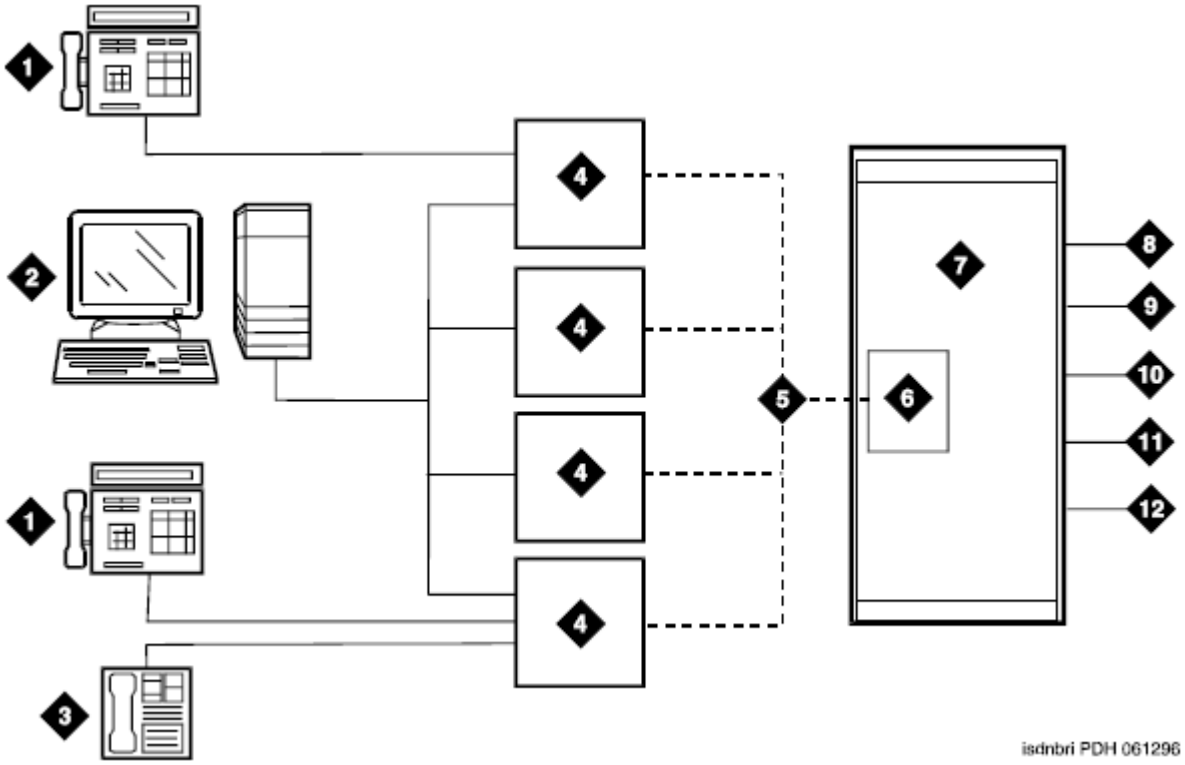


Figure 12: ISDN—BRI Personal Computer interface configuration (Group 2)

Table 5: Figure notes:

1. ISDN telephone
2. Personal Computer with application
3. Handset or Headset
4. BRI Interface card
5. 2B + D
6. ISDN Line (12-BRI-S-NT) circuit pack)
7. Avaya Server
8. PRI trunks
9. BRI stations
10. Interworking
11. DMI
12. Switch features

Personal Computer 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 Personal Computer/ISDN Interface cards on the same Personal Computer. 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.

Personal Computer Interface Security

There are two areas where unauthorized use might occur with this feature: unauthorized local use and remote access.

Security alert:

Unauthorized local use involves unauthorized users who attempt to make calls from a Personal Computer. The Personal Computer software has a security setting so users can place the Personal Computer in Security Mode when it is unattended. You also can assign Automatic Security so that the administration program on the Personal Computer is always active and runs in Security Mode. This mode is password-protected.

Security alert:

Remote access involves remote access to the Personal Computer over a data extension. Remote users can delete or copy Personal Computer files with this feature. You can password-protect this feature. See the *Avaya Toll Fraud and Security Handbook*, 555-025-600, for additional steps to secure your system and to find out about obtaining information regularly about security developments.

Administering a PC interface

Procedure

On the Station screen, set the **Type** field to `pc`.

Considerations for Personal Computer Interface

- Use the Function Key Module of the 7405D with Personal Computer Interface.
- BRI terminals normally are initializing terminals and require you to assign an SPID. The Personal Computer/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 Personal Computer/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 Personal Computer Interface. This terminal type is also non-initializing with no support of MIMs.

- Do not use telephones with data modules with the Personal Computer 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 Personal Computer 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 Personal Computer Interface. However, the 7404D with Personal Computer cartridge can be used, but only with Group 1 configurations.

Wideband Switching

Wideband Switching provides the ability to dedicate 2 or more ISDN-PRI B-channels or DS0 endpoints for applications that require large bandwidth. It provides high-speed end-to-end communication between endpoints where dedicated facilities are not economic or appropriate. ISDN-BRI trunks do not support wideband switching.

Wideband Switching supports:

- High-speed video conferencing
- WAN disaster recovery
- Scheduled batch processing (for example, nightly file transfers)
- LAN interconnections and imaging
- Other applications involving high-speed data transmission, video transmission, or high bandwidth

Detailed description of Wideband Switching

ISDN-PRI divides a T1 or E1 trunk into 24 (32 for E1) channels, where one channel is used for signaling, and all others for standard narrowband communication. Certain applications, like video conferencing, require greater bandwidth. You can combine several narrowband channels into one wideband channel to accommodate the extra bandwidth requirement. Communication Manager serves as a gateway to many types of high-bandwidth traffic. In addition, DS1 Converter circuit packs are used for wideband switching at DS1 remote EPN locations. They are compatible with both a 24-channel T1 and 32-channel E1 facility (transmission equipment). They support circuit-switched wideband connections (NxDS0) and a 192 Kbps packet channel.

Wideband Switching channel type descriptions

The following table provides information on Wideband Switching channel types.

Channel Type	Number of Channels (DSOs)	Data Rate
H0 (T1 or E1)	6 (grouped 4 (T1) or 5 (E1) quadrants of 6 B-channels each)	384 Kbps
H11 (T1 or E1)	24 (on T1 - all 24 B-channels, with the D-channel not used; on E1 - B-channels 1 to 15, and 17 to 25, and B-channels 26 to 31 unused)	1536 Kbps
H12 (E1 only)	30 (B-channels 1 to 15 and 17 to 31)	1920 Kbps
NxDS0 (T1)	2-24	128 to 1536 Kbps
NxDS0 (E1)	2-31	128 to 1984 Kbps

Wideband switching channel allocation

For standard narrowband communication, ISDN-PRI divides a T1 or E1 trunk as follows:

- T1 trunks are divided into 23 information channels are 1 signaling channel
- E1 trunks are divided into 30 information channels, 1 signaling channel, and 1 framing channel

Certain applications, like video conferencing, require greater bandwidth. You can combine several narrowband channels into one wideband channel to accommodate the extra bandwidth requirement. Communication Manager serves as a gateway to many types of high-bandwidth traffic. In addition, DS1 converters are used for wideband switching at remote locations.

Performed using one of the three allocation algorithms: fixed, flexible, or floating.

- Fixed allocation — Provides contiguous-channel aggregation. The starting channel is constrained to a predetermined starting point. (Used only for H0, H11, and H12 calls.)
- Flexible allocation — Allows a wideband call to occupy non-contiguous positions within a single T1 or E1 facility (NxDS0).
- Floating allocation — Enforces contiguous-channel aggregation. The starting channel is not constrained to a predetermined starting point (NxDS0).

Wideband Switching video application example

A typical video application uses an ISDN-PRI interface to DS0 1 through 6 of the line-side facility. The figure on page 414 shows an example.

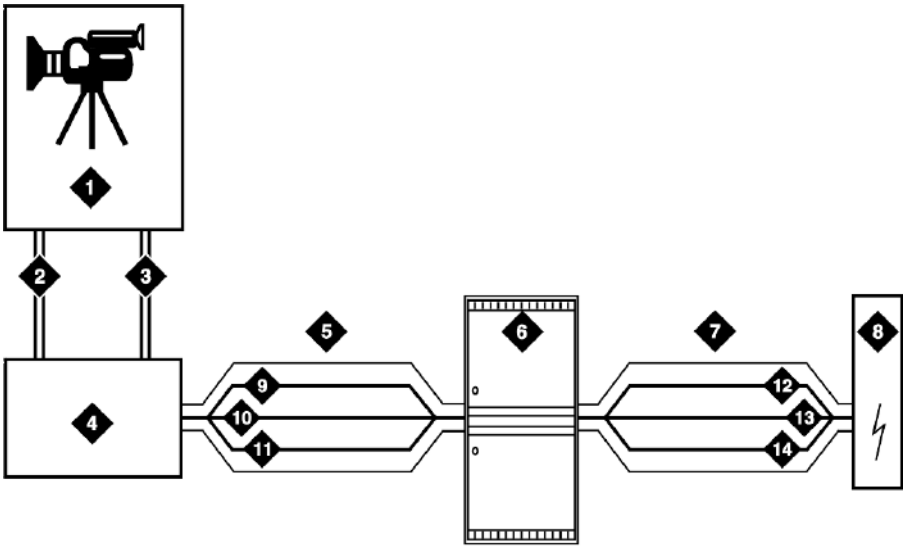


Figure 13: Typical video broadband application

Table 6: Figure notes:

1. Video application
2. Port 1
3. Port 2
4. ISDN terminal adaptor
5. Line-side ISDN-PRI
6. Avaya Server
7. ISDN or ATM-CES trunk
8. Network
9. DS0 24 D-channel
10. DS0 23 unused
11. DS0 1-6 wideband
12. DS0 24 D-channel
13. DS0 7-23 narrow bands
14. DS0 1-6 wideband

ISDN-PRI terminal adapters with Wideband Switching

For Wideband Switching with non-ISDN-PRI equipment, you can use an ISDN-PRI terminal adapter. ISDN-PRI terminal adapters translate standard ISDN signaling into a form that can be used by the endpoint application, and vice versa. The terminal adapter also must adhere to the PRI-endpoint boundaries as administered on Communication Manager when handling both incoming applications to the endpoint and outgoing calls.

The terminal adapter passes calls to and receives calls from the line-side ISDN-SETUP messages. These messages indicate the data rate and the specific B-channels (DS0) to be used. The terminal adapter communicates all other call status information by way of standard ISDN messages. For more information, see *DEFINITY® Line-Side ISDN Primary Rate Interface Technical Reference*.

Line-side T1 or E1 ISDN-PRI facilities with Wideband Switching

A line-side T1 or E1 ISDN-PRI facility is comprised of a group of DS0s. In this context, these DS0s are also called channels. T1 facilities have 23 B-channels and a single D-channel. E1 facilities have 30 B-channels, 1 D-channel, and a framing channel. Data flows bidirectionally across the facility between the server that is running Communication Manager and the ISDN-PRI terminal adapter.

PRI endpoints with Wideband Switching

A PRI-endpoint (PE) is a combination of DS0 B-channels on a line-side ISDN-PRI facility to which an extension is assigned.

A PE can support calls of lower bandwidth. In other words, a PE that has a width of six DS0 channels can handle a call of one channel of 64 Kbps, up to and including six channels totaling 384 Kbps. Also, a PE can support calls on nonadjacent channels. For example, an endpoint application that is connected to a PE that is defined as using B-channels 1 through 6 of an ISDN-PRI facility could use B-channels 1, 3, and 5 successfully to originate a call.

If the PE is administered to use flexible channel allocation, the algorithm for offering a call to the PE starts from the first DS0 that is administered to the PE. Since only one active call is permitted on a PE, contiguous B-channels are always selected unless one or more B-channels are not in service.

A PE remains in service unless all the B-channels are out of service. In other words, if B-channel 1 is out of service and the PE is five B-channels wide, the PE can still handle a wideband call of up to four B-channels wide. A PE can only be active on a single call at any given time. That is, the PE is considered to be idle, active or busy, or out of service.

One facility can support multiple separate and distinct PEs within a single facility. Non-overlapping contiguous sets of B-channel DS0s are associated with each PE.

Universal digital signal level 1 board

The universal digital signal level 1 (UDS1) board is the interface for line-side and network facilities that carries wideband calls.

Wideband Switching nonsignaling endpoint applications

Wideband Switching can also support configurations that use nonsignaling, non-ISDN-PRI line-side T1 or E1 facilities. The endpoint applications are the same as those that are defined for configurations with signaling.

Data service unit/channel service unit with Wideband Switching

The device service unit (DSU)/channel service unit (CSU) passes the call to the endpoint application. Unlike terminal adapters, the DSU/CSU does not have signaling capability.

Note:

No DSU/CSU is needed if the endpoint application has a fractional T1 interface.

Line-side (T1 or E1) facility with Wideband Switching

This facility, like the ISDN-PRI facility, is composed of a group of DS0s (24 for a T1 facility and 32 for an E1 facility; both T1 and E1 use 2 channels for signaling purposes). Line-side facilities are controlled solely from the server or Avaya 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 Server. These endpoints simply transmit and receive wideband data when the connection is active.

Note:

Communication Manager can determine if the connection is active, but this does not necessarily mean that data is actually coming across the connection.

A WAE is treated as a single endpoint and can support only one call. If all DS0s comprising a wideband access endpoint are in service, then the wideband access endpoint is considered in service. Otherwise, the wideband access endpoint is considered out of service. If an in-service wideband access endpoint has no active calls on its DS0s, it is considered idle. Otherwise, the wideband access endpoint is considered busy.

Multiple WAEs are separate and distinct within the facility and endpoint applications must be administered to send and receive the correct data rate over the correct DS0s. An incoming call at the incorrect data rate is blocked.

Wideband Switching guidelines and examples

This section examines wideband and its components in relation to the following specific customer usage scenarios:

- Data backup connection
- Scheduled batch processing
- Primary data connectivity
- Networking

Wideband Switching data backup connection

Using Wideband Switching for data transmission backup provides customers with alternate transmission paths for critical data in the event of primary transmission path failure.

Wideband Switching scheduled batch processing

Scheduled batch processing applications are used for periodic database updates, such as retail inventory, or distributions, such as airline fare schedules. These updates are primarily done after business hours and are often referred to as “nightly file transfers”. Wideband meets the

high bandwidth requirements at low cost for scheduled batch processing. With Wideband, the dedicated-access bandwidth for busy-hour switching traffic can be used for these applications after business hours. Thus, no additional bandwidth costs are incurred.

The non-ISDN backup data connection is also appropriate for scheduled batch processing applications. Administered Connections are used to schedule daily or weekly sessions that originate from this application.

Wideband Switching primary data connectivity

Permanent data connections are well suited for Communication Manager when ISDN-PRI endpoints are used. Permanent data connections, such as interconnections between local area networks (LANs), are always active during business hours. The ISDN end-to-end monitoring and the ability of the endpoint to react to failures provide for critical availability of data. With ISDN, endpoints can detect network failures and initiate backup connections through the server. ISDN endpoints can also establish additional calls when extra bandwidth is needed.

Any failures that Communication Manager does not automatically restore are signaled to the endpoint application. The endpoint application can initiate backup data connections over the same PRI endpoint. Communication Manager routes the backup data connections over alternate facilities if necessary.

Wideband Switching networking

All wideband networking is over ISDN-PRI facilities, and the emulation of ISDN-PRI facilities by ATM-CES. Wideband networking may also connect to a variety of networks, other services of domestic interexchange carriers, private line, RBOC services, and services in other countries.

Wideband Switching ISDN-PRI trunk groups and channel allocation

Only ISDN-PRI trunks, and the emulation of ISDN-PRI trunks by ATM-CES, support wideband calls to the network. The bandwidth requirements of wideband calls necessitate modification of the algorithms by which trunks look for clear channels.

The following sections describe the search methods, and the relationship of those methods to the available wideband data services.

Facility lists and Wideband Switching

The system always sends a wideband call over a single trunk group and a single DS1 facility (or other ISDN-PRI-capable facility). Since a trunk group can contain channels (trunk members) from several different DS1 facilities, the system maintains a facility list for each trunk group.

A facility list orders the trunk members based on signaling group. If the system is using non-facility associated signaling groups with multiple DS1 facilities, the system sorts trunk members in that signaling group according to the interface identifier assigned to the corresponding DS1 facility.

When searching for available channels for a wideband call placed over a given trunk group, the system starts with the channels in the lowest-numbered signaling group with the lowest interface identifier. If the system cannot find enough channels in a given signaling group with that interface identifier, it checks the next higher interface identifier. If no more interface identifiers are available

in the current signaling group, the system moves its search to the channels in the next higher signaling group.

For example, if three facilities having signaling group/interface identifier combinations of 1/1, 1/2, and 2/1 were associated with a trunk group, then a call offered to that trunk group would search those facilities in the order as they were just listed. Also note that since trunks within a given facility can span several trunk groups, a single facility can be associated with several different trunk groups.

Given this facility list concept, the algorithms have the ability to search for trunks, by facility, in an attempt to satisfy the bandwidth requirements of a given wideband call. If one facility does not have enough available bandwidth to support a given call, or it is not used for a given call due to the constraints presented in the following section, then the algorithm searches the next facility in the trunk group for the required bandwidth (if there is more than one facility in the trunk group).

In addition to searching for channels based on facilities and required bandwidth, Port Network (PN) preferential trunk routing is also employed. This PN routing applies within each algorithm at a higher priority than the constraints put on the algorithm by the parameters listed later in this section. In short, all facilities that reside on the same PN as the originating endpoint are searched in an attempt to satisfy the bandwidth of a given call, prior to searching any facilities on another PN.

Direction of trunk/hunting within facilities

You can tell the system to search for available channels in either ascending or descending order. These options help you reduce glare on the channels because the system can search for channels in the opposite direction to that used by the network. If an ISDN trunk group is not optioned for wideband, then a cyclical trunk hunt based on the administration of trunks within the trunk group is still available.

H11 channels

When a trunk group is administered to support H11, the algorithm to satisfy a call requiring 1,536 Kbps of bandwidth uses a fixed allocation scheme. That is, the algorithm searches for an available facility using the following facility-specific channel definitions:

- T1: H11 can only be carried on a facility without a D-channel being signaled in an NFAS arrangement (B-channels 1-24 are used).
- E1: Although the 1,536 Kbps bandwidth could be satisfied using a number of fixed starting points (for example, 1, 2, 3, and so forth), the only fixed starting point being supported is 1. Hence, B-channels 1-15 and 177-25 always are used to carry an H11 call on an E1 facility.

If the algorithm cannot find an available facility within the trunk that meets these constraints, then the call is blocked from using this trunk group. In this case, the call can be routed to a different trunk group preference via Generalized Route Selection (GRS), at which time, based on the wideband options administered on that trunk group, the call would be subject to another hunt algorithm (that is, either the same H11 algorithm or perhaps an N x DS0 algorithm described in a later paragraph).

Note that on a T1 facility, a D-channel is not considered a busy trunk and results in a facility with a D-channel always being partially contaminated. On an E1 facility, however, a D-channel is not

considered a busy trunk because H11 and H12 calls can still be placed on that facility; an E1 facility with a D-channel and idle B-channels is considered an idle facility.

H12 channels

Since H12 is 1,920 Kbps, which is comprised of 30 B-channels, a 1,920-Kbps call can be carried only on an E1 facility. As with H11, the hunt algorithm uses a fixed allocation scheme with channel 1 being the fixed starting point. Hence, an H12 call is always carried on B-channels 1 through 15 and 17 through 31 on an E1 facility, as the following table shows. When the system is offered any other call other than a 1,536-Kbps call, the algorithm behaves as it does when H11 is optioned.

		DS0s that comprise each channel	
Facility	**ISDN interface**	**H11**	**H12**
T1	23B + D	-	-
T1	24B (NFAS)	1-24	-
E1	30B + D	1 through 15, 17 through 25	1 through 15, 17 through 31
E1	31B (NFAS)	1 through 15, 17 through 25	1 through 15, 17 through 31

H0 channels

When a trunk group is administered to support H0, the algorithm to satisfy a call requiring 384 Kbps of bandwidth also uses a fixed allocation scheme. Unlike the H11 fixed scheme which only supports a single fixed starting point, the H0 fixed scheme supports 4 (T1) or 5 (E1) starting points. The H0 algorithm searches for an available quadrant within a facility based on the direction of trunk or hunt administered. If the algorithm cannot find an available quadrant within any facility allocated to this trunk group, then the call is blocked from using this trunk group. Again, based on GRS administration, the call might route to a different trunk group preference and be subject to another algorithm based on the wideband options administered.

Note that a D-channel is considered a busy trunk and results in the top most quadrant of a T1, B-channels 19 to 24, always being partially contaminated. This is *not true* for NFAS.

If this H0 optioned trunk group is also administered to support H11, H12, or N x DS0, then the system also attempts to preserve idle facilities. In other words, when offered a narrowband, H0, or N x DS0 call, the system searches partially-contaminated facilities before it searches to idle facilities.

N x DS0 channels

For the N x DS0 multi-rate service, a trunk group parameter determines whether a floating or a flexible trunk allocation scheme is to be used. The algorithm to satisfy an N x DS0 call is either floating or flexible.

- Floating (Contiguous) — In the floating scheme, an N x DS0 call is placed on a contiguous group of B-channels large enough to satisfy the requested bandwidth without any constraint being put on the starting channel (that is, no fixed starting point trunk).
- Flexible — In the flexible scheme, an N x DS0 call is placed on any set of B-channels as long as the requested bandwidth is satisfied. There is absolutely no constraint such as

contiguity of B-channels or fixed starting points. Of course, as with all wideband calls, all the B-channels comprising the wideband call must reside on the same ISDN facility.

Regardless of the allocation scheme employed, the N x DS0 algorithm, like the H11 and H12 algorithms, attempts to preserve idle facilities when offered B, H0, and N x DS0 calls. This is important so that N x DS0 calls, for large values of N, have a chance of being satisfied by a given trunk group. However, if one of these calls cannot be satisfied by a partially-contaminated facility and an idle facility exists, a trunk on that idle facility is selected, thus contaminating that facility.

There are additional factors to note regarding specific values of N and the N x DS0 service:

- N = 1 — this is considered a narrowband call and is treated as any other voice or narrowband-data (B-channel) call.
- N = 6 — if a trunk group is optioned for both H0 and N x DS0 service, a 384-kbps call offered to that trunk group is treated as an H0 call and the H0 constraints apply. If the H0 constraints cannot be met, then the call is blocked.
- N = 24 — if a trunk group is optioned for both H11 and N x DS0 service, a 1,536-kbps call offered to that trunk group is treated as an H11 call and the H11 trunk allocation constraints apply.
- N = 30 — if a trunk group is optioned for both H12 and N x DS0 service, a 1,920-kbps call offered to that trunk group is treated as an H12 call and the H12 trunk allocation constraints apply.

Wideband Switching glare and blocking prevention

Wideband Switching glare prevention

Glare occurs when both sides of an ISDN interface select the same B-channel for call initiation. For example, a user side of an interface selects the B-channel for an outgoing call and, before Communication Manager receives and processes the SETUP message, the server also selects the same B-channel for call origination. Since any single wideband call uses more channels, the chances of glare are greater. With proper and careful administration, glare conditions can be reduced.

To reduce glare probability, the network needs to be administered so both sides of the interface select channels from opposite ends of facilities. This is called linear hunting, ascending or descending. For example, on a 23B+D trunk group, the user side could be administered to select B-channels starting at channel 23 while the network side would be administered to start selecting at channel 1. Using the same example, if channel 22 is active but channel 23 is idle, the user side should select channel 23 for re-use.

Wideband Switching blocking prevention

Blocking occurs when an insufficient number of B-channels are available to make a call. Narrowband calls require only one channel, so blocking is less likely than with wideband calls that require multiple B-channels. Blocking also occurs for wideband calls when bandwidth is unavailable in the appropriate format, such as fixed, floating, or flexible.

To reduce blocking, Communication Manager selects trunks for both wideband calls and narrowband calls to maximize the availability of idle fixed channels for H0, H11, and H12 calls, and idle floating channels for N x DS0 calls that require a contiguous bandwidth. The strategy for preserving idle channels depends on the channel type. The chances for blocking are reduced if you use a flexible algorithm, assuming that the algorithm is supported on the other end.

The following table describes the blocking strategy for the different channel types.

Channel type	Blocking minimization strategy
H0	Preserve idle quadrants
H11	Preserve idle facilities
H12	Preserve idle facilities
Flexible N x DS0	Preserve idle facilities
Floating N x DS0	Preserve idle facilities as first priority

Administering Wideband Switching

About this task

Before you start, you need a DS1 Converter circuit pack.

Procedure

1. On the Access Endpoint screen, administer all fields.
2. On the PRI Endpoint screen, administer all fields.
3. On the ISDN Trunk Group screen, administer all fields.
4. On the Route Pattern screen, administer all fields.

Considerations for Wideband Switching

- For wideband switching with non-ISDN-PRI equipment, you can use an ISDN-PRI terminal adapter.

Interactions for Wideband Switching

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

Administered Connections

Administered Connections provides call initiation for wideband access endpoints (WAEs). All Administered Connections that originate from WAEs use the entire bandwidth that is administered for WAE. The destination of an Administered Connection can be a PRI endpoint.

Automatic Circuit Assurance (ACA)

ACA treats wideband calls as single-trunk calls so that a single ACA-referral call is made if an ACA-referral call is required. The call is on the lowest B-channel that is associated with the wideband call.

Call Coverage

A WAE cannot be administered as a coverage point in a call-coverage path.

Call Detail Recording (CDR)

When CDR is active for the trunk group, all wideband calls generate CDR records. The CDR feature flag indicates a data call, and CDR records contain bandwidth and Bearer Capability Class (BCC).

Call Forwarding

You must block Call Forwarding through Class of Service (COS).

Call Management System (CMS) and Basic Call Management System (BCMS)

Wideband calls can be carried over trunks that are measured by CMS and BCMS. Wideband endpoints are not measured by CMS and BCMS.

Call Vectoring

PRI endpoints use a vector directory number (VDN) to dial. For example, PRI endpoint 1001 dials VDN 500. VDN 500 points to Vector 1. Vector 1 can point to other PRI endpoints such as route-to 1002, or route-to 1003, or busy.

Certain applications use Call Vectoring. When an incoming wideband call hunts for an available wideband endpoint, the call can point to a VDN, that sends the call to the first available PRI endpoint.

Class of Restriction (COR)

COR identifies caller and called-party privileges for PRI endpoints. Administer the COR so that account codes are not required. Forced entry of account codes (FEAC) is turned off for wideband endpoints.

Class of Service (COS)

COS determines the class of features that a wideband endpoint can activate.

Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS)

FAS and NFAS with or without D-Channel Backup requires administration by way of signaling groups for trunk-side wideband interfaces.

Facility Busy Indication

You can administer a busy-indicator button for a wideband-endpoint extension, but the button does not accurately track endpoint status.

Facility Test Calls

Use Facility Test Calls to perform loop-back testing of the wideband call facility.

Generalized Route Selection (GRS)

GRS supports wideband BCC to identify wideband calls. GRS searches a route pattern for a preference that has wideband BCC. Route preferences that support wideband BCC also support other BCCs for different call types to share the same trunk group.

CO Trunk (TTC - Japan) Circuit Pack

The CO Trunk (TTC - Japan) circuit pack cannot perform wideband switching. No member of the circuit pack should be a member of a wideband group.

CallVisor Adjunct-Switch Applications Interface

CallVisor Adjunct-Switch Applications Interface (ASAI) links Communication Manager and adjunct applications. The interface allows adjunct applications to access switching features and supply routing information to Communication Manager. CallVisor ASAI improves Automatic Call Distribution (ACD) agents' call handling efficiency by allowing an adjunct to monitor, initiate, control, and terminate calls on the Avaya Server. The CallVisor ASAI interface can be used for Inbound Call Management (ICM), Outbound Call Management (OCM), and office automation or 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 or Internet Protocol transport (Avaya LAN Gateway).

CallVisor ASAI messages and procedures are based on the ITU-T Q.932 international standard for supplementary services. The Q.932 Facility Information Element (FIE) carries the CallVisor ASAI requests and responses across the interface. An application program can access CallVisor ASAI services by supporting the ASAI protocol or by using a third-party vendor application programming interface (API).

ASAI configuration example

For a simple ASAI configuration example, see the figure on page 423.

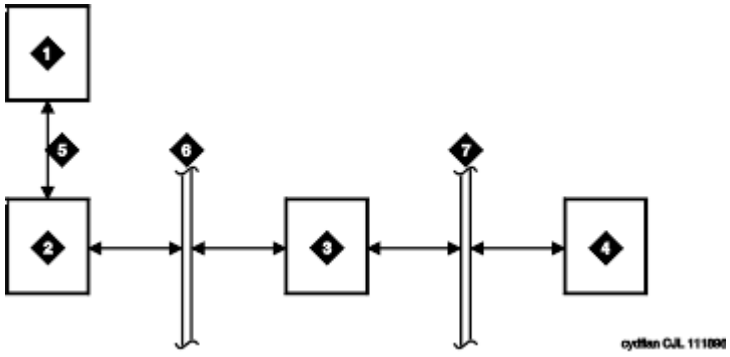


Figure 14: ASAI Switch Interface Link — BRI Transport

Table 7: 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 *Communication Manager ASAI Technical Reference*, 555-230-220.

Considerations for ASAI

- If your system has an expansion cabinet (with or without duplication), ASAI resources should reside on the system's Processor Cabinet.

Interactions for ASAI

See *Communication Manager ASAI Technical Reference*, 555-230-220.

Setting up ASAI

Procedure

1. Type `add cti-link n`, where *n* is a CTI link number from 1 to 64.
2. Press `Enter`.

   The system displays the CTI Link screen.
3. In the **Type** field, type:
   - `asai-ip` if the adjunct platform is not CentreVu Computer Telephony.
   - `adj-ip` if the adjunct platform is CentreVu Computer Telephony.
4. Save the changes.

CallVisor ASAI setup

CallVisor Adjunct-Switch Applications Interface (ASAI) can be used in the telemarketing and help-desk environments. It is used to allow adjunct applications to monitor and control resources in Communication Manager.

Preparing to set up ASAI

Procedure

On the System Parameters Customer-Options (Optional Features) screen, verify that the:

- **ASAI Link Core Capabilities** field is `y`. If not, go to the Avaya Support website at http://support.avaya.com.
- **Computer Telephony Adjunct Links** field is `y` if the adjunct is running the CentreVu Computer Telephony.

Setting up ASAI

Procedure

1. Type `add cti-link` *n*, where *n* is a CTI link number from 1 to 64.
2. Press `Enter`.

   The system displays the CTI Link screen.
3. In the **Type** field, type:
   - `asai-ip` if the adjunct platform is not CentreVu Computer Telephony.
   - `adj-ip` if the adjunct platform is CentreVu Computer Telephony.
4. Save the changes.

Chapter 21: Collecting Call Information

Call information collection

Call Detail Recording (CDR) collects detailed information about all incoming and outgoing calls on specified trunk groups. If you use Intra-switch CDR, you can also collect information about calls between designated extensions on Communication Manager. Communication Manager sends this information to a printer or to some other CDR output device that collects call records and that might also provide reports.

You can have a call accounting system directly connected to your Avaya server running Communication Manager. If you are recording call details from several servers, Communication Manager can send the records to a collection device for storage. A system called a poller can then take these records and send them to the call accounting system. The call accounting system sorts them, and produces reports that you can use to compute call costs, allocate charges, analyze calling patterns, detect unauthorized calls, and keep track of unnecessary calls.

Requirements for administering call accounting

The call accounting system that you use might be sold by Avaya, or it might come from a different vendor. You need to know how your call accounting system is set up, what type of call accounting system or call detail recording unit you are using, and how it is connected to the server running Communication Manager. You also need to know the format of record that your call accounting system requires.

⚠ Caution:

When migrating a platform from a legacy system to a Linux-based system of Communication Manager 3.0 or newer, where both the old and new systems use CDR, ensure that the older CDR parsing scripts correctly use all of the characters identified in each of the fields contained in the applicable format table (see the Format Tables in the *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205).

Setting up CDR example

About this task

In this example, we are going to establish Call Detail Recording (CDR) for all calls that come in on trunk group 1 (our CO trunk). We are going to set up CDR so that any call that is handled by an attendant produces a separate record for the attendant part of the call.

Procedure

1. Log in to Communication Manager System Administration Terminal (SAT) interface.
2. At the command prompt, type `change trunk-group n`.
3. In the **CDR Reports** field, type `y`.

   When you enable CDR Reports, Communication Manager creates call records for calls made over this trunk group.
4. Select `Enter` to save your changes.
5. Type `change system-parameters cdr`.
6. In the **CDR Format** field, type `month/day`.

   This determines how the date appears on the header record.
7. In the **Primary Output Format** field, type `Unformatted`.

   This is the record format that your call accounting system requires. Check with your call accounting vendor to determine the correct record format for your system.
8. In the **CDR Retention (Days)?** field, type the number of days for which you want to retain the logs. You can enter a value between 1 to 20.

   The Capacity Scan discovers the sum of the files collected for the last 20 days, plus the current file being collected today exceeds the internally-computed maximum capacity of twenty times 20 megabytes. So Communication Manager's Capacity Scan will delete the oldest file of the twenty aged files. This leaves 19 days of previously collected CDR files plus the current file. So, even though you type `20` for the log retention, it will only have 19 collected days plus the current day.
9. In the **Use Legacy CDR Formats** field, type `y` to use CDR formats from Communication Manager 3.1 and earlier.
10. Type `n` to use formats from Communication Manager 4.0 and later.

    For more information, see *Avaya Aura® Communication Manager Screen Reference*.
11. 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.
12. 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.
13. 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.
14. 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.

You can also administer Communication Manager to produce separate records for calls that are conferenced or transferred. This is called Call Splitting. There are many other variations that you can administer for CDR.

For additional information on Call Detail Recording (CDR), see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Intra-switch CDR administration

Call detail recording generally records only those calls either originating or terminating outside the server running Communication Manager. There might be times when you need to record calls between users on the local server. Intra-switch CDR lets you track calls made to and from local extensions.

Setting up intra-switch CDR example

Procedure

1. In this example, we administer Communication Manager to record all calls to and from extensions 5100, 5101, and 5102.
2. Type **`change system-parameters cdr`** and select `Enter`.
3. In the **intra-switch CDR** field, enter `y` and select `Enter` to save your changes.
4. Type **`change intra-switch-cdr`** and select `Enter`.
5. In the first three available slots, enter `5100`, `5101`, and `5102`.
6. Select `Enter` to save your changes.

   Communication Manager will now produce call records for all calls to and from these extensions, including those that originated on the local server.

   For more information, see *Avaya Aura® Communication Manager Screen Reference*.

Account Code call tracking

You can have your users to enter account codes before they make calls. By doing this, you can have a record of how much time was spent on the telephone doing business with or for a particular client.

Setting up Account Code call tracking example

About this task

In this example, we are going to set up the system to allow the user at extension 5004 to enter a 5-digit account code before making a call.

Procedure

1. Enter **change system-parameters cdr**.
2. In the **CDR Account Code Length** field, type `5` and select `Enter` to save your changes.
3. Assign an account button on the **Station** screen for extension 5004.
4. Provide your users with a list of account codes to use.
5. You can also assign a feature access code and give this to your users.

Forced Entry of Account Codes

Forced Entry of Account Codes is another form of account code dialing. You can use it to allow certain types of calls only with an account code, to track fax machine usage by account, or just to make sure that you get account information on all relevant calls.

Preparing to administer Forced Entry of Account Codes

Procedure

Verify that Forced Entry of Account Codes is enabled on the System Parameters Customer-Options (Optional Features) screens.

If it is not, go to the Avaya Support website at http://support.avaya.com.

Administering Forced Entry of Account Codes example

About this task

In this example, we administer the system to force users in our North American office to enter an account code before making international calls.

Procedure

1. Type **change system-parameters cdr** and select `Enter`.
2. In the **Force Entry of Acct Code for Calls Marked on Toll Analysis Form** field, type `y`.
3. In the **CDR Account Code Length** field, type `5` and select `Enter` to save your changes.
4. Type **change toll 0**.

   Press `Enter`.

5. The system displays the Toll Analysis screen.
6. In the first available **Dialed String** field, type `011`.

   This is the international access code for this office.
7. In the **Total Min** and **Max** columns, type `10` and `18`, respectively.

   This is the minimum and maximum number of digits the system will analyze when determining how to handle the call.
8. In the **Toll List** and **CDR FEAC** columns, type `x`.
9. Press `Enter` to save your changes.

   You can also establish a class of restriction with **Forced Entry of Account Codes** set to `y`, and assign this class of restriction (COR) to trunks or other facilities that you want to restrict. With this method, all users with this COR must enter account codes before making any outgoing trunk calls. See Class of Restriction in *Avaya Aura® Communication Manager Screen Reference* for more information.

Public network Call-Charge Information administration

Communication Manager provides two ways to receive information from the public network about the cost of calls. Note that this service is not offered by the public network in some countries, including the US.

- Advice of Charge (AOC, for ISDN trunks) collects charge information from the public network for each outgoing call. Charge advice is a number representing the cost of a call; it might be recorded as either a charging or currency unit.
- Periodic Pulse Metering (PPM, for non-ISDN trunks) accumulates pulses transmitted from the public network at periodic intervals during an outgoing trunk call. At the end of the call, the number of pulses collected is the basis for determining charges.

For more information about AOC and PPM, see Call Charge Information in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Preparing to administer public network call-charge information

Procedure

You need to request either AOC or PPM service from your network provider.

In some areas, your choice might be limited. Go to the Avaya Support website at http://support.avaya.com to determine the type of service you need and open a service request.

Note:

This service is not offered by the public network in some countries, including the U.S.

Collecting call charge information over ISDN example

About this task

In this example, we administer the system to provide Advice of Charge over an existing ISDN trunk group, at the end of a call. This information will appear on CDR reports.

Procedure

1. Enter **`change trunk-group 2`**.
2. In the **CDR Reports** field, type `y`.

   This ensures that the system displays the AOC information on the CDR report.
3. Verify that **Service Type** is `public-ntwrk`.
4. In the **Supplementary Service Protocol** field, enter `a`.
5. The **Charge Advice** field, enter `end-on-request`.

   This ensures that Communication Manager will place one request for charge information. This reduces the amount of information passed to Communication Manager and consumes less processor time than other options.
6. Select `Enter` to save your changes.

Charge Advice for QSIG trunks administration

Use the QSIG Supplementary Service - Advice of Charge feature to extend charging information from the public network into the private network. The charging information that many service providers supply is extended from a gateway enterprise system to the end user's enterprise system. The charging information can then be displayed on the user's desktop.

Information can be extended and displayed either:

- At intervals during the call and at the end of the call, or
- Only at the end of the call

QSIG stands for Q-Signaling, which is a common channel signal protocol based on ISDN Q.931 standards and used by many digital telecommunications systems. Only charge information received from the public network with ETSI Advice of Charge, and Japan Charge Advice is extended into the QSIG private network.

Administering Charge Advice for QSIG

Procedure

1. On the Trunk Group screen, for Group Type **ISDN**, <tab> to the **Charge Advice** field.
2. Select from the following options:
   - during-on-request - to request that charging information be provided at intervals during a call, and also at the end of the call
   - end-on request - to request that charging information be provided only at the end of a call

- none - no charging information will be requested for the trunk group

Note:

Receipt of charge advice on the QSIG trunk group is also dependent on Charge Advice administration at the PSTN trunk group involved on the call, and whether charges are received from the public network.

3. On the **Trunk Group** screen, administer the **Decimal Point** field.
   - period (.) -This is the default. If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a period as the decimal point.
   - comma (,) - If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a comma as the decimal point.

   If the received charge contains no decimals, no decimal point is displayed (that is, the administered decimal point is ignored for charge information received with no decimals). On an upgrade from a QSIG trunk group with the **Decimal Point** field administered as `none`, the field defaults to **period**.

Receiving call-charge information over non-ISDN trunks example

About this task

In this example, we will administer an existing Direct Inward and Outward Dialing (DIOD) trunk to receive PPM from the public network.

Procedure

1. Type **`change trunk-group 3`**.

   The system displays the Trunk Group screen with existing administration for this trunk group. Click the numbered page tabs or **Next Page** to find fields that appear on subsequent pages of the Trunk Group screen.

2. In the **CDR Reports** field, type `y`.

   This ensures that the system displays the PPM information on the CDR report.

3. In the **Direction** field, enter `two-way`.
4. Click **Next Page** to find the **PPM** field.
5. In the **PPM** field, enter `y`.
6. In the **Frequency** field, enter `50/12`.

   This is the signal frequency (in kHz). The frequency you will use depends on what the circuit pack you use is able to accept. See Tone Generation in *Avaya Aura® Communication Manager Screen Reference*, for more information.

7. In the **Administrable Timers** section, set the **Outgoing Glare Guard** timer to `5` seconds and select **Enter** to save your changes.

8. You also need to ensure that the values of the **Digital Metering Pulse Minimum**, **Maximum** and **Value** on the DS1 Circuit Pack screen are appropriate to the values offered by your service provider.

Viewing Call Charge Information example

About this task

Communication Manager provides two ways for you to view call-charge information: on a telephone display or as part of the Call Detail Recording (CDR) report. From a display, users can see the cost of an outgoing call, both while the call is in progress and at the end of the call.

In this example, we administer extension 5040 to be able to view the charge of a call in progress. The charges will appear in currency units (in this case, Lira) on the telephone display of the user.

Procedure

1. Enter `change trunk-group 2`.
2. Click **Next Page** until you see the **Trunk Features** section.
3. In the **Charge Conversion** field, enter `200`.

   This indicates that one charge unit sent from the service provider is equal to 200 units, in this case, Lira.
4. In the **Decimal Point** field, enter `none`.
5. In the **Charge Type** field, enter `Lira` and select `Enter` to save your changes.
6. Enter `change system-parameters features`.
7. In the Charge Display Update Frequency (seconds) field, enter `30` and select `Enter` to save your changes.

   Frequent display updates might have considerable performance impact.
8. Now assign extension 5040 a **disp-chrg** button to give this user the ability to control the charge display.

   See Adding Feature Buttons for more information.

   If you want end users to control when they view this information, you can assign a display button that they can press to see the current call charges. If you want call charges to display automatically whenever a user places an outgoing call, you can set **Automatic Charge Display** to `y` on the COR screen.

Survivable CDR detailed description

The Survivable CDR feature is used to store CDR records to a server's hard disk. For Survivable Core and Survivable Remote Servers, the Survivable CDR feature is used to store the CDR records generated from calls that occur when a Survivable Remote or Survivable Core Server is controlling one or more gateways or port networks. The Survivable CDR feature provides the ability to store CDR records on the hard disk of the server.

When the Survivable CDR feature is enabled, the CDR records are saved in a special directory named `/var/home/ftp/CDR` on the server's hard disk. The CDR adjunct retrieves the Survivable CDR data files by logging into the server and copying the files to its own storage device. The CDR adjunct uses a special login that is restricted to only accessing the directory where the CDR records are stored. After all the files are successfully copied, the CDR adjunct deletes the files from the server's hard disk and processes the CDR records in the same manner that it does today.

Note:

This feature is available on main servers and Survivable Core Servers that are Communication Manager Release 5.0 and later releases only. It is available on Survivable Remote platforms running Communication Manager 4.0 and later.

The CDR adjunct must poll each main, Survivable Remote Server, and Survivable Core Server regularly to see if there are any new data files to be collected. This is required even when a Survivable Remote or Survivable Core Server is not controlling a gateway or a port network because the CDR adjunct has no way of knowing if a Survivable Remote or Survivable Core Server is active.

The Survivable CDR feature uses the same CDR data file formats that are available with legacy CDR.

Files for Survivable CDR

When Survivable CDR is enabled, the server writes the CDR data to files on the hard disk instead of sending the CDR data over an IP link. The Survivable CDR feature creates two types of CDR data files: a Current CDR data file that the server uses to actively write CDR data and a set of archive files containing CDR data that the server collected earlier but has not yet been collected and processed by the CDR adjunct. The naming convention for both file types are similar. However the name of the Current CDR file is always prefixed by a "C-" (for more information, see File naming conventions for Survivable CDR). The CDR Current file remains active until one of the following events happen:

- The server's system clock reaches 12:00 midnight.
- The Current CDR file reaches or exceeds 20 megabytes. A 20 megabyte file may contain up to 140K CDR records depending on the CDR format used.

- A filesync, a reset system 2 (cold restart), or a reset system 4 (reboot) occurs.

After one of the above events occur the following actions take place:

- The Current CDR file is closed and it becomes an archive CDR file.
- The file permissions change from `read/write (rw)` for root and read only for members of the CDR_User group to:
  - Owner (root): `Read/Write/Execute (rwx)`
  - Group (CDR_User): `Read/Write (rw-)`
  - World: `none (---)`
- The “C-” prefix is removed from the front of the file name
- For a main server, a new Current CDR file is created
- For a Survivable Remote or Survivable Core Server, a new Current CDR file is created only if the Survivable Remote or Survivable Core Server is controlling one or more gateways or port networks.

File naming conventions for Survivable CDR

The Survivable CDR data files have the following naming conventions:

`tssssss-cccc-YYMMDD-hh_mm`

where:

- `t` is populated with an L for a Survivable Remote Server, an E for a Survivable Core Server, or an S for a main server
- `ssssss` is populated with the least significant six digits of the System ID or SID. The SID is a unique number in the RFA license file used to identify the system. The SID for a server can be viewed by using one of the following methods:
  - Use the **`statuslicense -v`** BASH command.
  - Use the command **`display system-parameters customer-options`** on the SAT.
- `cccc` is populated with the least significant four digits of the Cluster ID (CL ID) or Module ID (MID). To display the MID for the server:
  - Use the **`statuslicense -v`** BASH command.
- `YY` is populated with the two digit number of the year the file was created.
- `MM` is populated with the two digit number of the month the file was created.
- `DD` is populated with the two digit day of the month the file was created.
- `hh` is populated with the hour of the day the file was created based on a 24 hour clock.

- `mm` is populated with the number of minutes after the hour when the file was created.

The Current CDR file uses the same naming convention except the name is prefixed with a “C-”.

Survivable CDR file removal

You can remove CDR files by:

The Survivable CDR feature

The Survivable CDR feature on the main, Survivable Remote Server, or Survivable Core Server automatically removes the oldest CDR data achieve file anytime the number of archived files exceed 20. The Current CDR file is not an archived file on the hard disk and, therefore, cannot be counted in the 20 files.

CDR adjunct

In a normal operating environment, the CDR adjunct has the responsibility to delete the CDR data files after they are copied and verified that they are correct.

Survivable CDR file access

The administrators can use a special user group called CDR_User to identify all users authorized to access the CDR storage directory. The archived CDR files are stored in `/var/home/ftp/CDR`.

Administering Survivable CDR

Procedure

1. Create a new user account for CDR adjunct access and permissions to retrieve CDR data files, see Creating a new user account.
2. Enable CDR storage on the hard disk, see Administering Survivable CDR for the main server.
3. If using this feature on the main server: Administer the **Primary Output Endpoint** field on the main’s **`change system-parameters cdr`** SAT form to be DISK, see Administering Survivable CDR for the main server.

   When using Survivable CDR, only the **Primary Output Endpoint** field is available. Administration of the **Secondary Output Endpoint** field is blocked.
4. If you are using this feature on a Survivable Remote Server and a Survivable Core Server: Administer the **Enable CDR Storage on Disk** field on the change survivable-processor

screen, see Administering Survivable CDR for a Survivable Remote or Survivable Core Server.

Creating a new CDR user account

About this task

For the CDR adjunct to access the CDR data files, a new user account must be created on the main server. The new account is pushed to the Survivable Remote and/or Survivable Core Server when a filesync is performed.

Procedure

1. On the Server Administration Interface, click **Administrator Accounts** under the Security heading.
2. On the Administrator Accounts page, enter the login ID for the new user in the **Enter Login ID or Group Name** field.
3. Click the **Add Login** radio button and then click **Submit**.
4. On the Administrator Logins -- Add Login page, enter the data in the table on page 437 in each field.

Table 8: 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

Table continues…

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

5. Click **Add** to create the new user account.

Administering Survivable CDR for the main server

Procedure

On the **system-parameters cdr** screen:

a. **Enable CDR Storage on Disk?**: Possible entries for this field are yes or no.

   Entering yes in this field enables the Survivable CDR feature for the main, Survivable Remote Server, and Survivable Core Server. If this field is set to no, the CDR functionality remains as legacy CDR.

b. **Primary Output Endpoint**: Possible entries for this field are CDR1, CDR2, and DISK.

   For the main server, the **Primary Output Endpoint** field must be set to DISK. When Survivable CDR is administered as Disk on the **Primary Output Endpoint** field, the **Secondary Output Endpoint** field is blocked.

Administering Survivable CDR for a Survivable Remote or Survivable Core Server

About this task

Note:

The Survivable CDR feature is administered on the main server for the Survivable Remote and Survivable Core Servers.

Important:

A Survivable Remote or Survivable Core Server only stores Survivable CDR records if it is administered to support Survivable CDR and if it is controlling one or more gateways or port networks.

Procedure

1. On the **system-parameters cdr** screen:

   Enable CDR Storage on Disk: Possible entries for this field are yes or no.

Entering yes in this field enables the Survivable CDR feature for the main, Survivable Remote, and Survivable Core Servers. If this field is set to no, the CDR functionality remains legacy CDR.

2. On the Survivable-processor screen:
   a. **Service Type**: The **Service Type** field must be set to CDR1 or CDR2 to enable entries to the **Store to Dsk** field.
   b. **Store to Dsk**: Enter `y` to enable Survivable CDR for this Survivable Remote or Survivable Core Server.

      When the **Service Type** field is set to CDR1 or CDR2 and the **Store to Dsk** field is set to yes, all CDR data for the specific Survivable Remote or Survivable Core Server being administered will be sent to the hard disk rather than output to an IP link. Survivable Remote or Survivable Core Server will only store CDR records to hard disk when the Survivable Remote or Survivable Core Server is controlling a gateway or port network.

Important:

You must complete the Survivable Processor screen for each Survivable Remote or Survivable Core Server that uses the Survivable CDR feature.

Note:

The **Enable** field for a given line in the change survivable-processor screen must be set to *o* (overwrite) to change that line.

Chapter 22: Assigning multiple call arrangement bridge to a Station

About this task

This supports customers who want to migrate from CS1000 to Communication Manager and retain the existing MADN MCA operation or who wish to implement the new multiple call arrangement bridge capability.

Procedure

1. Enter `change station xxxx`.
2. Click **Next Page** until you see a page with available buttons.
3. Tab down to the available entry and enter: **brdg-appr**.
4. At the **B:** field, enter the value `a`.

Chapter 23: User Administration

User Administration management

For information about User Administration to manage user accounts, see *Administering Avaya Aura® System Manager*.

Chapter 24: Communication Manager objects

For information about Communication Manager objects, see *Administering Avaya Aura® System Manager*.

Chapter 25: Endpoints

For managing endpoints, see *Administering Avaya Aura® System Manager*.

Chapter 26: Templates

For information about templates, see *Administering Avaya Aura® System Manager*.

Chapter 27: Overview of Inventory Management

You can use the Inventory Management feature to configure Avaya Aura® System Manager to discover specific devices within the network. By using the Inventory Management feature, you can manage the SNMP access parameters that are used for the inventory collection process.

By using Inventory Management, you can do the following:

- Detect or discover your network that includes subnets and nodes.
- Discover your network by using Simple Network Management Protocol (SNMP)

For more information about the following, see the *Administering Avaya Aura® System Manager* and *SNMP Administration and Reference* guides:

- Discovering elements
- Discovering SRS and SCS servers
- Creating profiles
- Overview of Inventory Management

Chapter 28: Messaging

Subscriber Management

With System Manager, you can perform messaging system administration activities, such as add, view, edit, and delete subscribers. You can also administer mailboxes, and modify mailbox settings for a messaging system.

System Manager supports:

- Communication Manager 5.0 and later and
- Avaya Aura® Messaging 6.0 and later

Adding a subscriber

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select one or more messaging systems from the list of Messaging Systems.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions**, and **Miscellaneous** sections.
7. Complete the **Add Subscriber** page and click **Commit** to add the subscriber.

Note:

If you select more than one Messaging or Modular Messaging from the list of messaging systems, and then click **New**, the system displays the Add Subscriber page with the first Messaging or Modular Messaging in context.

Related links

Subscribers (Avaya Aura Messaging) field descriptions on page 449

Editing a subscriber

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. From the Subscriber List, choose the subscriber you want to edit.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields in the **Edit Subscriber** page.
8. Click **Commit** to save the changes.

Related links

Subscribers (Avaya Aura Messaging) field descriptions on page 449

Viewing a subscriber

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Select the subscriber you want to view from the Subscriber List.
6. Click **View**.

Note:

You cannot edit any field on the View Subscriber page.

Related links

Subscribers (Avaya Aura Messaging) field descriptions on page 449

Deleting a subscriber

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.

2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Select the subscriber you want to delete from the Subscriber List.
6. Click **Delete**.

   The system displays a confirmation page for deleting the subscriber.
7. Confirm to delete the subscriber or subscribers.

   Note:

   You cannot delete a subscriber associated with a user through mailbox management. You can delete the user associated subscribers only through User Profile Management.

Subscriber list

The subscriber list displays all subscribers in a messaging version, such as Messaging, Communication Manager Messaging, or Modular Messaging. You can apply filter to each column in the subscriber list. You can also sort subscribers according to each of the column in the subscriber list. You must refresh the page to view the information that is updated after the last synchronization.

Name	Description
Name	The name of the subscriber.
Mailbox Number	The mailbox number of the subscriber.
Email Handle	The email handle of the subscriber.
Telephone Number	The telephone number of the mailbox.
Last Modified	The time and date when the subscriber details were last modified.
User	The name of the user to which the subscriber is associated.
System	The messaging system of the subscriber.

Filtering subscribers

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.

3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Click the **Filter: Enable** option in the Subscriber List.
6. Filter the subscribers according to one or multiple columns.
7. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

   Note:

   The table displays only those subscribers that match the filter criteria.

Subscribers (Avaya Aura® Messaging) field descriptions

Name	Description
System	The name of the messaging system.
Template	The messaging template of a subscriber template.
Last Name	The last name of the subscriber.
First Name	The first name of the subscriber.
Mailbox Number	The full mailbox number of a subscriber, including the site group and site identifiers, and the short mailbox number. Subscribers use mailbox numbers to log on to their respective mailbox. For a PBX subscriber, the mailbox number ranges from 3 to 10 digits in length. Other local subscribers use this field to address messages to the PBX subscriber. For a Multisite system subscriber, the mailbox number is up to 50 digits in length. Ensure that the mailbox number is: • Within the range of mailbox numbers assigned to your system. • Unassigned to another local subscriber. • A valid length on the local computer. This is a mandatory field on the Add Subscriber pages for all types of messaging systems.

Table continues…

Name	Description
Password	The default password the subscriber must use to log in to the mailbox. The password can be from 3 to 15 digits and adhere to system policies set on the Avaya Aura® Messaging server.
Save as Template	Saves your current settings as a template.

Basic Information

Name	Description
Class Of Service Name	The name of the class of service (CoS) for this subscriber. CoS controls subscriber access to many features and provides general settings, such as mailbox size. The value that you select must be available in the messaging system.
Community ID	The default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Numeric Address	The unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
Time zone	The time zone for Avaya Aura® Messaging time subscribers. The value must be in the standardized name format, America/Phoenix. Otherwise, the system sets the Avaya Aura® Messaging subscriber time zone to the System Manager server time zone.
PBX Extension	The primary telephone extension of the subscriber. For a Multisite system subscriber, this number is up to 50 digits in length.
Site	The name of the site. Avaya Aura® Messaging includes a site named **Default**. Change the default name when you set site properties for the first time.

Subscriber Directory

Field	Description
Email Handle	The name that the system displays before the computer name and domain in the subscriber's email address.

Table continues…

Field	Description
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]).
Common Name	The display name of the subscriber in address book listings, such as those for email client applications. The name can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII version of name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.
Pronounceable Name	The pronounceable name of the user. The name of a user, info mailbox, or distribution list might not follow the pronunciation rules of the primary language for your system. To increase the likelihood of the Speech Recognition feature recognizing the name, spell the name as you would pronounce the name. For example, if the primary language of your system is English, spell Dan DuBois as Dan Doobwah. You can enter an alternative name for the user. For example, William Bell might also be known as Bill Bell. If you enter William in the First name field, Bell in the Last name field, and Bill Bell in the Pronounceable name field, the speech engine recognizes both William Bell and Bill Bell.
Include in Auto Attendant directory	The option to add the messaging system to the auto attendant directory.

Subscriber Security

Name	Description
Expire Password	An option to set the password expiry. The options are: • **yes**: for password to expire • **no**: if you do not want your password to expire

Table continues…

Name	Description
Is Mailbox Locked?	The option to lock your mailbox. A subscriber mailbox can get locked after two unsuccessful login attempts. The options are: • **no**: To unlock your mailbox • **yes**: To lock your mailbox and prevent access to it

Mailbox Features

Name	Description
Personal Operator Mailbox	The mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber greeting.
Personal Operator Schedule	The option to specify when to route calls to the backup operator mailbox. The default value is **Always Active**.
TUI Message Order	The order in which the subscriber hears the voice messages. The options are: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.

Table continues…

Name	Description
Intercom Paging	The intercom paging settings for a subscriber. The options are: • **paging is off**: Disables intercom paging for this subscriber. • **paging is manual**: Callers can page the subscriber with Subscriber Options or TUI if the subscriber can modify. • **paging is automatic**: Callers automatically page the subscriber with TUI.
VoiceMail Enabled	The option to specify if a subscriber can receive messages, email messages, and call-answer messages from other subscribers. The options are: • **yes**: To create, forward, and receive messages. • **no**: To prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.
MWI enabled	The option to enable the message waiting indicator (MWI) light feature. The options are: • **No**: The user has a voice mailbox only. • **ByCOS**: CoS controls how the system enables MWI. The **MWI enabled** field overrides the MWI setting defined by the CoS to which the user is associated.

Secondary Extensions

Field	Description
Secondary Extension	One or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers. For Avaya Aura® Messaging 6.3, you can add a maximum eight secondary extensions.

Miscellaneous

Field	Description
Miscellaneous 1	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 2	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 3	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 4	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Saves all the changes.
Edit	Allows you to edit the fields.
Reset or **Clear**	Clears all changes.
Cancel	Returns to the previous page.

Chapter 29: Administering LDAP Directory Application

LDAP Directory Application overview

From Release 8.0, you need to install the Avaya Aura® AVP Utilities on same hardware where Communication Manager is installed. Use the LDAP Directory Application web pages to configure LDAP Directory Application to connect to an LDAP database and to customize the search experience of the user.

You can install Directory Application on the supported Avaya servers. For the list of supported servers, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

The 96xx, and 96x1 telephones use Wireless Markup Language (WML) browsers to browse LDAP databases.

96xx and 96x1 telephones URL configuration

You can configure the URL on 96xx and 96x1 telephones by using the WMLHOME property in the settings file. Use the following URLs:

- The URL for HTTP is: `http://<AVP Utilities IP address>/directoryclient/search.php`
- The URL for HTTPS is: `https://<AVP Utilities IP address>/directoryclient/search.php`

For more information on configuring WML browsers for the 96xx and 96x1 telephones, see *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide*.

Chapter 30: Administering IP DECT

IP DECT

Use the IP DECT (Digital Enhanced Cordless Telecommunications) feature to support an IP DECT system, an IP-based cordless telephony and messaging system for connection to private telephone exchanges.

Enabling multiple locations for IP DECT

About this task

Important:

Perform this task only if you need to enable the multiple locations feature in Communication Manager system.

Procedure

1. Enter `display system-parameters customer-options`.
2. Click **Next** until you see the **Multiple Locations** field.
3. Ensure that the **Multiple Locations** field is set to y.

   Note:

   If the **Multiple Locations** field is set to n, multiple locations is not enabled for the IP DECT feature. Go to the Avaya Support website at http://support.avaya.com for assistance.
4. Select **Enter** to exit the screen.

Verifying system capacities

Procedure

1. Enter `display capacity`.
2. Click **Next** until you see the **Total Licensed Capacity** section.
3. Ensure that the following fields display the current information:
   - **XMOBILE Stations**: Total number of X-Mobile stations including the IP DECT stations.
   - **ISDN DECT**: Current number of ISDN-based DECT X-Mobile stations.

- **IP DECT**: Current number of IP-based DECT X-Mobile stations.

4. Select **Enter** to exit the screen.

Assigning the codec

Procedure

1. Enter `change ip-codec-set n` or `change ip-media-parameters n`, where *n* is the IP codec set number.

   The system displays the IP MEDIA PARAMETERS screen.

   Note:

   The codec set that has to be configured in the IP Network Region must be linked to this IP MEDIA PARAMETERS screen.

2. Fill in the following fields:

   - **Audio Codec**: G.711 a-law and u-law (for 10, 20, 30 ms packets), G.729/G.729a/G.729b/G.729ab (for 10, 20, 30, 40, 50, 60 ms packets), and G.723 (for 30, 60 ms packets) depending on the audio codec used for this codec set.

     Note:

     When using G.729 codecs, for outgoing packets, the legacy IP DECT system (ADMM) either uses G.729A or G.729AB.

   - **Silence Suppression**: `y` or `n` depending on the codec you have set.

     The ADMM system does not support silence suppression for G.729 or G.729A codecs.

   - **Frame Per Pkt**: `2`.
   - **Media Encryption**: `none`, `srtp-aescm-128`, or `srtp-aescm-256`.

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

   For information on administering the IP codec sets, see the Administering IP Codec sets section of *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

   For information on additional parameters to control media stream usage for fax and data transport modes, see *Avaya Aura® Communication Manager Screen Reference*.

Configuring the network region

Procedure

1. Enter `change ip-network-region n`, where *n* is the network region.

   Note:

   The Far-end Network Region that has to be configured in the signaling-group must be linked to this codec.

2. Fill in the following fields:
   - **Codec Set**: 1 to 7 depending on the codec set to be used for the network region.
   - **RSVP Enabled**: `n`.
3. Click **Next** until you see the **Inter Network Region Connection Management** section.

   Avaya recommends you to use the same codec set which you already assigned, see Assigning the codec task.

   For information on administering the IP network regions, see the Administering IP network regions section of *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.
4. Select **Enter** to save your changes.

Configuring the trunk group

Procedure

1. Enter `add trunk-group n`, where *n* is the trunk group number.

   Note:

   You must administer this trunk group to use an H.323 signaling group of x-mobility type of DECT.
2. Ensure that the **Group Type** field is set to `isdn`.
3. Fill in the following fields:
   - **Direction**: `two-way`.
   - **Carrier Medium**: `H.323`.
   - **Service Type**: `tie`.
4. Click **Next** until you see the **Trunk Parameters** section.
5. Fill in the following fields:
   - **Codeset to Send Display**: `0`.
   - **Supplementary Service Protocol**: `a`.
   - **Digit Handling (in/out)**: `overlap/enbloc`.
   - **Format**: Type the numbering format.

     The numbering format no need to be any specific type. For example, IP trunk to the IP DECT can have Private numbering format.
6. Click **Next** until you see the **Trunk Features** section.
7. Fill in the following fields:
   - **NCA-TSC Trunk Member**: 1 or higher for carrying Message Waiting Indication (MWI) facility.

- **Send Name**: `y`.
- **Send Calling Number**: `y`.
- **Send Connected Number**: `y`.

8. Click **Next** until you see the **Group Member Assignments** section.
9. Add trunk group members to the numbered **Group Member Assignments**.

Note:

The IP DECT supports maximum of 255 simultaneous calls. The IP DECT can choose another available trunk if administered.

Note:

Instead of adding the trunk group members on the **Group Member Assignments**, you can set the **Member Assignment Method** field to auto.

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

Configuring the signaling group

Procedure

1. Enter `add signaling-group n`, where *n* is the signaling group number.
2. Ensure that the **Group Type** field is set to H.323.
3. Fill in the following fields:
   - **Max number of NCA TSC**: 1 or higher.
   - **Max number of CA TSC**: 1 or higher.
   - **Trunk Group for NCA TSC**: Type the number of the previously administered or associated trunk group.
   - **Trunk Group for Channel Selection**: Type the number of the previously administered or associated trunk group.
   - **TSC Supplementary Service Protocol**: `a`.
   - **X-Mobility/Wireless Type**: `DECT`.
   - **Location for Routing Incoming Calls**: `blank` or the location of the ADMM or RFS.

     Note:

     Administer the **Location for Routing Incoming Calls** field only when the multiple locations feature is enabled for IP DECT.
   - **Near-end Listen Port**: Port of the CLAN or PE.
   - **Far-end Listen Port**: Port of the ADMM or RFS.
   - **Far-end Network Region**: Point to the associated network region.

- **Calls Share IP Signaling Connection**: `n`.
- **Interworking Message**: `PROGress`.
- **Enable Layer 3 Test**: `y` for IP trunk supervision.

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

Configuring the station

Procedure

1. Enter `add station n`, where *n* is the extension.
2. Ensure that the **Type** field is set to XMOBILE.
3. Ensure that the **XMOBILE Type** field is set to IPDECT.
4. Fill in the following fields:
   - **Message Lamp Ext**: Type the station number.
   - **Display Module**: `y`.
   - **Message Waiting Type**: ICON, DISP, or NONE depending on the MWI message requirement.
   - **Length of Display**: Type the proper length for each of the handset.

     Avaya recommends that the **Length of Display** field must be set to 16x2.
   - **Mobility Trunk Group**: Type the appropriate trunk group that use the H.323 signaling groups.

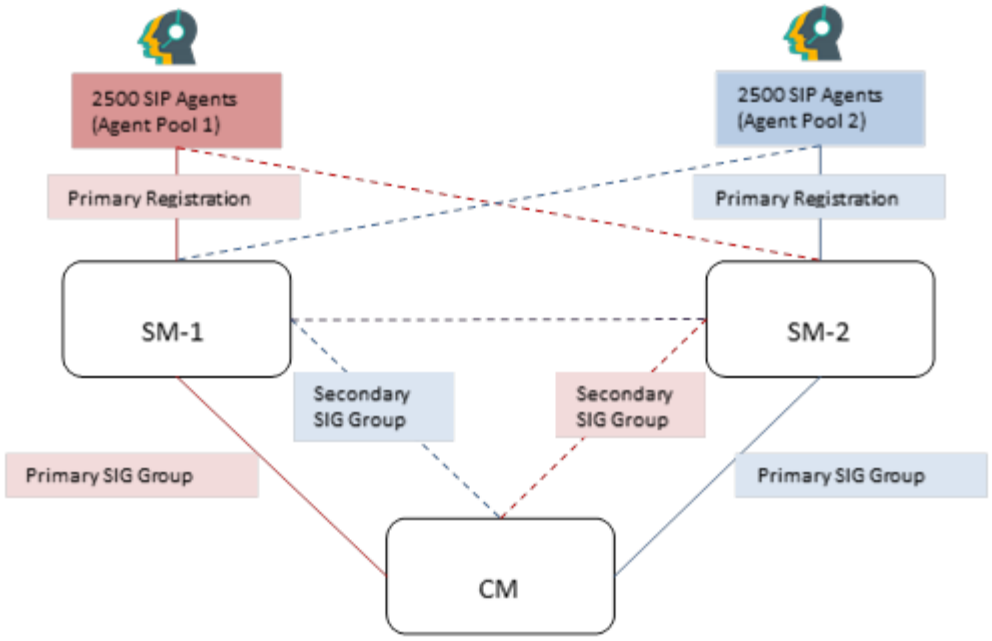
     Note:

     You must not change the value of the **Mobility Trunk Group** field while a call is active.
   - **Mapping Mode**: `both`.
5. Select **Enter** to save your changes.

Chapter 31: Administering SIP trunk optimization

SIP trunk optimization

The SIP trunk optimization feature eliminates the need for provisioning trunks for redundancy. This feature frees up trunks so that the available trunks can be used by SIP agents, SIP stations, or PSTN bound SIP trunk calls. Following illustration explains the problem of trunk consumption due to redundancy.

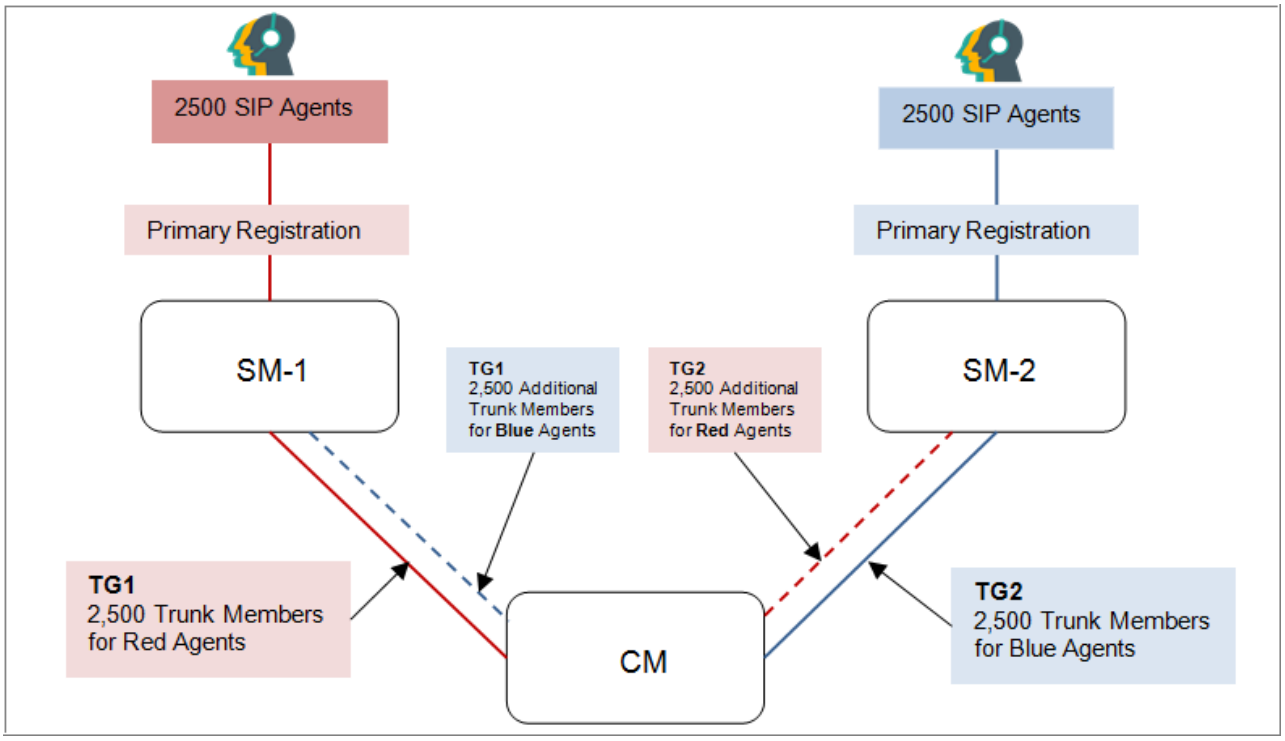


Above figure provides two scenarios:

- First scenario: When the connection between Communication Manager and Session Managers work fine.
- Second scenario: When the connection between Communication Manager and Session Manager fails.

In the first scenario, if Communication Manager wants to reach the red agents (agent pool 1), it can do so by utilizing the red trunk between Communication Manager and Session Manager-1.

Similarly, if Communication Manager wants to reach the blue agents (agent pool 2), it can do so by utilizing the blue trunk between Communication Manager and Session Manager-2.



In the second scenario, administering additional trunks provide a solution for giving service to red and blue agents, but introduces few other problems.

- The additional trunk members administered for redundancy remain unused in the first scenario, when entity links to Session Manager-1 and Session Manager-2 are in service.
- Double the number of trunks need to be provisioned to cover a rarely occurring second scenario. Given the limited trunk members on Communication Manager, using trunks for redundancy reduces the trunks required for actual traffic.
- Routing and administration of route-patterns becomes complex.

For provisioning connectivity to Session Manager-1 and Session Manager-2, Communication Manager has to create two signaling groups:

- Signaling group to Session Manager-1: Near-End as procr and Far-End as Session Manager-1
- Signaling group to Session Manager-2: Near-End as procr and Far-End as Session Manager-2

Each signaling must have 5000 trunks provisioned with Session Manager-1 and 5000 trunks to be provisioned with Session Manager-2 as described earlier.

SIP trunk optimization feature allows each signaling group to point to multiple Session Managers. In this particular case, a signaling group will point to both Session Manager-1 and Session Manager-2. This is achieved by pointing the signaling group to a cluster of Session Managers. An SM cluster can have as many as 28 Session Managers. With a Session Manager cluster, it is assumed that all Session Managers share similar configuration and any Session Manager can route a call to the far end station or far end trunk.

The ability of signaling group to point to both Session Managers reduces the required trunks by half to be administered on Communication Manager while achieving full redundancy. If the link to the Session Manager-1 fails, then the Signaling group uses the link to Session Manager-2 to route all the outgoing traffic. The effect of having one signaling group pointing to multiple Session Managers is as follows:

- Signaling group remains in service if at least one Session Manager administered in the cluster is reachable.
- Trunk group remains in service and all members administered in the trunk group can be used to deliver traffic.
- For example, trunk group with 5000 members in the first scenario can service 2500 agents on Session Manager-1 and 2500 agents on Session Manager-2. The same trunk group with 5000 members can services 2500 agents on Session Manager-1 and 2500 agents on Session Manager-2 through the link between Communication Manager and Session Manager-2, if the connectivity between Communication Manager and Session Manager-1 goes down. Even if Session Manager-1 goes down and all agents move to Session Manager-2, the same 5000 members will be able to reach all the 5000 agents.

Additional enhancements made in SIP trunk optimization feature are as follows:

- Number of trunk members have been increased to 9,999 for SIP trunk groups.
- Number of SIP agents have been increased to 10,000.
- System wide trunk members have been increased to 30,000.
- Measured trunks have been increased to 30,000.
- TLS connections for SIP have been increased to 56 from the current value of 32, to support 28 Session Managers. Because, two links are required to support each Session Manager.
- SIP Station form directly points to its Primary and Secondary Session Manager to support 28 Session Managers, because two links are required to support each Session Manager. For more details on the capacities, see *Avaya Aura® Communication Manager System Capacities Table*.
- Look Ahead Routing feature is deprecated for SIP station calls if routed over clustered signaling group.
- Route pattern can now specify a network region.

Related links

Adding Session Managers to a cluster on page 463
Administering the number of members on a trunk group on page 464

Adding Session Managers to a cluster

About this task

The Cluster Session Manager form in the Communication Manager SAT interface allows you to add up to 28 Session Managers.

Procedure

1. In a SAT session, enter `change cluster session manager`.

2. Enter the names of the Session Managers that you want the cluster to point to.

Related links

SIP trunk optimization on page 461

Administering the number of members on a trunk group

Procedure

1. In a SAT session, enter `change trunk group`.
2. In the **Number of Members** field, enter a required value.

   You can enter up to 9,999 trunk members. If you want to change the value to 256 or more, then the **Number Assignment Method** field value must set to auto.

Related links

SIP trunk optimization on page 461

Chapter 32: Certificate Management

Certificate Management provides for support of importing new identity certificates and trusted CA certificates with enhanced signatures, such as SHA2 and 2048 key length.

Certificate Management enables receiving and validating both existing certificates with SHA1-1024 signature and new certificates with SHA2-2048 signature.

Certificate installation activity is a maintenance activity and must be performed during maintenance window when there is no call traffic running on the Communication Manager system. Performing installation activity on live system can yield undesired system behavior like service disruption and system overload.

Communication Manager uses four application directories to hold certificates.

Application Directory	Service/Interface	Peer entity	Usage
C	Communication Manager telephony	Session Manager another peer CM server, AES, CM Duplication link, FIleSync links, H.248 gateways and 96x1 H.323 phone.	SIP trunk, H.323 over TLS and others
W	Administration Web Server	PC	Communication Manager Web Administration
R	Remote logging	Syslog server and general Services access	logging and services access
A	Authentication, Authorization and Accounting (AAA) services (for example, LDAP)	External AAA server	Administration accounts authentication

Related links

Generating a CSR on page 472
Generating a CSR when third-party signed certificate is unavailable on page 473

Identity Certificates

Overview

Each Communication Manager is installed with a unique identity certificate for Communication Manager Telephony service, including the SIP TLS link. This certificate is unique for each customer, and is secure. Three methods exist for certificate creation/signing:

1. Import a 3rd party hosted certificate pair (Trusted CA chain and the Identity cert)
2. Create a signed cert on SMGR and import to CM
3. Use CM's Certificate Signing Request (CSR) and point to SMGR's CA or to some other CA for signing.

You should generate 2048 bits and SHA-2 hash identity certificates with your CA for all Communication Manager services/interfaces, including Telephony service.

The Communication Manager Messaging service has its non-unique identity certificate that is signed by Avaya SIP Product Certificate Authority, and automatically installed during installation. Communication Manager Web Server is the same.

Each service or interface can only have ONE identity certificate, but one identity certificate may be copied into multiple repositories.

Displaying a certificate

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Server/Application Certificates**.
3. Select a certificate from the list that has been, and click **Display**.

Addition of an identity certificate

About this task

Communication Manager allows the certificate file received from CA in PEM format or in PKCS#12 format. There are two methods for Communication Manager to get the identity certificate from CA directory.

- Generate a Certificate Signing Request (CSR) file and submit the CSR file to CA. By using the CSR request, CA issues a signed certificate file in PEM format (no private key contained) or in PKCS#12 format (with or without private key contained).
- Request CA to generate a private/public key pair and the certificate directly and the certificate can only be delivered in a PKCS#12 format file, which contains both of the private and public keys.

Adding an identity certificate for Simplex server

About this task

To add the signed Identity certificate received from CA to identity certificate repositories, upload the pem format file or PKCS#12 format file to `/var/home/ftp/pub` directory first.

The signed Identity certificate can be a single certificate (self-signed root certificate) or a also include the certificate chain with the chain of trust that reverts back to a trusted certificate. Communication Manager supports chained identity certificate.

You must have already installed the CA certificate that is provided by the CA and has been used to authenticate your certificate or the chained certificate, to CM trusted certificate repositories. This CA certificate must be trusted by all the Communication Manager services/interfaces that the identity certificate is applied for. If the CA certificate is not trusted by a Communication Manager service/interface, the installation of identity certificate for this service will fail, and Communication Manager prompts an error message.

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Server/Application Certificates**.
3. Click **Add**.
4. Enter the file name of the certificate (that has been loaded into) in the `/var/home/ftp/pub` folder.

   The file must contain a certificate (that has been loaded into) chain to add. The certificate must be either a PKCS#12 file or a file in pem format.
5. Enter the password of the certificate. This is necessary, since the signed certificate file will be encrypted with this password so that it is not transported in the clear as the administrator is importing the certificate.
6. Click **Open to validate the certificate**.

   After successful verification, the Server/Application Certificates - Add page shows the issued-to, issued-by, and date of expiration information for each of the added certificates in the chain. If the file does not contain a valid certificate, the system displays an error message instead of the certificate content.
7. Select the appropriate repositories in which the certificate needs to be installed.
8. Click **Add**.

   Communication Manager does not needs to be restarted for the certificate to take effect.

Adding an identity certificate for a Duplex server

About this task

To add the signed identity certificate received from CA to identity certificate repositories, upload the pem format file or PKCS#12 format file to `/var/home/ftp/pub` directory first.

The signed Identity certificate can be a single certificate (self-signed root certificate) or include the certificate chain with the chain of trust that reverts to a trusted certificate. Communication Manager supports chained identity certificate.

You must have already installed the CA certificate that is provided by the CA and has been used to authenticate your certificate or the chained certificate, to CM trusted certificate repositories. This CA certificate must be trusted by all the Communication Manager services/interfaces that the identity certificate is applied for. If the CA certificate is not trusted by a Communication Manager service/interface, the installation of an identity certificate for this service fails, and Communication Manager prompts an error message.

Note:

Both the Communication Manager servers in Duplex system have their identity certificate, and the identity certificates must be installed on respective servers. You must install the identity certificates on both the Communication Manager servers.

However, the new certificates must be installed on the active server before doing an interchange.

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Server/Application Certificates**.
3. Click **Add**.
4. Enter the file name of the certificate (that is loaded into) in the `/var/home/ftp/pub` folder.

   The file must contain a certificate (that is loaded into) chain to add. The certificate must be a PKCS#12 file or a file in pem format.
5. Enter the password of the certificate. This is necessary since the signed certificate file is encrypted with this password so that it is not transported in the clear as the administrator is importing the certificate.
6. Click **Open to validate the certificate**.

   After successful verification, the Server/Application Certificates - Add page shows the issued-to, issued-by, and date of expiration information for each of the added certificates in the chain. If the file does not contain a valid certificate, the system displays an error message instead of the certificate content.
7. Select the appropriate repositories in which the certificate needs to be installed.
8. Click **Add**.

   Communication Manager does not needs to be restarted for the certificate to take effect.

Removing an identity certificate

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Server/Application Certificates**.
3. Select a certificate entry and click **Add**.

   The Server/Application Certificates – Remove page shows the file name, issued-to, issued by, date of expiration, and installed-in information for the first certificate in the selected certificate chain.
4. Select the appropriate repositories from which you want to remove the certificate.
5. Click **Remove**.

Copying an identity certificate

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Server/Application Certificates**.
3. Select a certificate entry and click **Copy**.

   The Server/Application Certificates - Copy page shows the certificate content of the first certificate in the chain along with a list of all other repositories from which you can select any combination.
4. Select the appropriate repositories from which you want to install the certificate.
5. Click **Copy** to install the selected certificate in the selected repositories.

   For each repository where the certificate is installed, the system overwrites or creates the `server.crt` and `server.key` files.

Trust certificates

Displaying a certificate

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Trusted Certificates**.
3. Select a certificate, and click **Display**.

Related links

Certificate Management on page 465

Adding a trusted certificate for Simplex server

About this task

A trusted certificate must be a Certificate Authority (CA) certificate. To add a trusted certificate to certificate repository, upload the pem format file to `/var/home/ftp/pub` directory.

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Trusted Certificates**.
3. Click **Add**.
4. Enter file name of the certificate in the `/var/home/ftp/pub` folder.
5. Click **Open to validate the certificate**.

   After successful verification, the Trusted Certificates – Add page shows the issued-to, issued-by, and date of expiration information for the added certificate.
6. Enter a file name to use to store the certificate.
7. Select the appropriate repositories in which the certificate needs to be installed.
8. Click **Add**.

   If you fail to install a certificate in one repository, it does not affect the installation in other repositories.

Related links

Certificate Management on page 465

Adding a trusted certificate for Duplex server

About this task

A trusted certificate must be a Certificate Authority (CA) certificate. To add a trusted certificate to certificate repository, upload the pem format file to `/var/home/ftp/pub` directory. Trusted certificate installation must be performed on the active Communication Manager server in a Duplex system pair.

Note:

There is NO need to copy the root CA cert file to the standby Communication Manager server. The root CA cert file is copied by Communication Manager's active server, as part of server synchronization, immediately after the CA cert was installed onto the active Communication Manager server.

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Trusted Certificates**.
3. Click **Add**.
4. Enter file name of the certificate in the `/var/home/ftp/pub` folder.
5. Click **Open to validate the certificate**.

   After successful verification, the Trusted Certificates – Add page shows the issued-to, issued-by, and date of expiration information for the added certificate.
6. Enter a file name to use to store the certificate.
7. Select the appropriate repositories in which the certificate needs to be installed.
8. Click **Add**.

   If you fail to install a certificate in one repository, it does not affect the installation in other repositories.

Related links

Certificate Management on page 465

Removing a certificate

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Trusted Certificates**.
3. Select a certificate entry and click **Remove**.
4. Select the appropriate repositories from which you want to remove the certificate.
5. Click **Remove**.

Related links

Certificate Management on page 465

Copying a certificate

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Trusted Certificates**.
3. Select a certificate entry and click **Copy**.
4. Select the appropriate repositories in which you want to install the selected certificate.

5. Click **Copy** to install the selected certificate in the selected repositories.

   For each repository where the certificate is installed, the system overwrites or creates the `server.crt` and `server.key` files.

Related links

Certificate Management on page 465

Generating a CSR

Procedure

1. On the Communication Manager SMI interface, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Certificate Signing Request**.
3. Enter the appropriate details in the fields.
4. Click **Generate**.

Related links

Certificate Management on page 465
Certificate Signing Request field descriptions on page 472

Certificate Signing Request field descriptions

Name	Description
Country Name	Enter a two-letter code to represent the country.
State or Province Name	Enter the name of the state or province where Communication Manager is located.
Locality Name	Enter the name of the city.
Organization Name	Enter the name of organization applying for the certificate.
Organization Unit	Enter the name of the organization unit applying for the certificate.
Common Name	Enter the name to identify Communication Manager or the specific service on Communication Manager that you are applying certificate for.
Signing Request Hashing Algorithm	Select one of the following: SHA-1, SHA-256 and SHA-512. It is recommended to select SHA-256 for higher security.
RSA Key Size	Select 1024 or 2048 key length. It is recommended to use 2048 for the RSA key length for higher security.

Table continues…

Name	Description
This is a CA certificate	Specify whether the certificate is a CA certificate. The system displays this field only on the main server. The main server may act as a sub-CA to sign certificate signing request from LSP or ESS servers. This type of CA certificate can only be installed in Communication Manager. Select Yes in this case. But LSP and ESS servers can request signed certificate from CA separately. Select No in this case, and your main CM server won't be the sub-CA.

Related links

Generating a CSR on page 472

Generating a CSR when third-party signed certificate is unavailable

If you do not have a third-party signed certificate, then you can have the CSR certificate signed from the System Manager.

In case of direct SIP trunks, if you are making a direct trunk between 2 Communication Managers having different System Managers, then the System Manager pem files should be exchanged in order to have the link working. For example, if you have a Communication Manager 7.0 and Communication Manager 7.1 with SIP direct link, then you need to have System Manager 7.0 pem file on Communication Manager 7.1, and Communication Manager 7.1 pem file on System Manager 7.0.

Note:

If you are using a duplex server, you must first install the certificate on a standby server. Later, you must interchange the server and apply the certificate on the new standby server. You must install the certificate on Enterprise Survivable Server (ESS) and Local Survivable Processor (LSP) separately.

Procedure

1. On the Communication Manager SMI, click **Administration** > **Server (Maintenance)**.
2. In the **Security** section, click **Certificate Signing Request**.
3. Enter the appropriate details in the fields.

   For more information, see the "Certificate Signing Request field descriptions" section.
4. Click **Generate Request**.
5. Copy the content between "BEGIN CERTIFICATE REQUEST" and "END CERTIFICATE REQUEST", and click **Continue**.
6. Log on to System Manager web interface, and navigate to **Security** > **Certificates** > **Authority**.

7. Click **RA Functions** > **Add End Entity**, and enter the required details.

   For more information, see the “Creating an end entitiy” section in *Administering Avaya Aura® System Manager*.
8. In the left navigation pane, click **Public Web**.
9. In the new window, click **Create Certificate from CSR**.
10. In the **Certificate enrollment from a CSR** page, enter the user name and password that you created in Step 7.
11. Paste the CSR content that you copied in Step 5.
12. To generate and download the certificate on to your local machine, click **OK**.
13. Go to Communication Manager SMI, and download the certificate from your local machine.
14. In the **Security** section, click **Server/Application Certificates**.
15. Click **Add**, and copy the certificate which was downloaded.
16. Click **Open**, and check **Communication Manager**.
17. Click **Add**.

Related links

Certificate Management on page 465

Chapter 33: Resources

Communication Manager documentation

The following table lists the documents related to Communication Manager. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® Communication Manager Overview and Specification	Provides an overview of the features of Communication Manager	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Security Design	Describes security-related issues and security features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager System Capacities Table	Describes the system capacities for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
LED Descriptions for Avaya Aura® Communication Manager Hardware Components	Describes the LED for hardware components of Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware requirements for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Survivability Options	Describes the system survivability options for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Core Solution Description	Provides a high level description for the solution.	Sales Engineers, Solution Architects
Maintenance and Troubleshooting		
Avaya Aura® Communication Manager Reports	Describes the reports for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides procedures to maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel

Table continues…

Title	Description	Audience
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides commands to monitor, test, and maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Alarms, Events, and Logs Reference	Provides procedures to monitor, test, and maintain Avaya servers, and describes the denial events listed on the Events Report form.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		
Administering Avaya Aura® Communication Manager	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network connectivity for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager SNMP Administration and Reference	Describes SNMP administration for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Avaya Aura® Communication Manager Server Options	Describes server options for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Data Privacy Guidelines	Describes how to administer Communication Manager to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation and Upgrading		
Deploying Avaya Aura® Communication Manager in Virtualized Environment	Describes the implementation instructions while deploying Communication Manager on VMware and Kernel-based Virtual Machine (KVM).	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Virtual Appliance	Describes the implementation instructions while deploying Communication Manager on Appliance Virtualization Platform.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Infrastructure as a Service Environment	Describes the implementation instructions while deploying Communication Manager on Amazon Web Services, Microsoft Azure, Google Cloud Platform.	Implementation Engineers, Support Personnel, Solution Architects

Table continues…

Title	Description	Audience
Deploying Avaya Aura® Communication Manager in Software-Only Environment	Describes the implementation instructions while deploying Communication Manager on a software-only environment.	Implementation Engineers, Support Personnel, Solution Architects
Upgrading Avaya Aura® Communication Manager	Describes instructions while upgrading Communication Manager.	Implementation Engineers, Support Personnel, Solution Architects
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Screen Reference	Describes the screens that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Special Application Features	Describes the special features that are requested by specific customers for their specific requirement.	Sales Engineers, Solution Architects, Avaya Business Partners, Support Personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.

2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support by Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in **Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
20970W	Introducing Avaya Device Adapter
20980W	What's New with Avaya Aura® Release 8.1
71200V	Integrating Avaya Aura® Core Components
72200V	Supporting Avaya Aura® Core Components
20130V	Administering Avaya Aura® System Manager Release 8.1
21450V	Administering Avaya Aura® Communication Manager Release 8.1

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Appendix A: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) for any software update. For example, a PCN must accompany a service pack or an update that must be applied universally. Avaya issues a product-support notice (PSN) when there is no update, service pack, or release fix, but the business unit or Avaya Services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a work around for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at https://support.avaya.com.

   If the Avaya Support website displays the login page, enter your SSO login credentials.
2. On the top of the page, click **DOCUMENTS**.
3. On the Documents page, in the **Enter Your Product Here** field, type the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select the appropriate filters as per your search requirement.

   For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new services packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to http://support.avaya.com and search for “Avaya Support Web Tips and Troubleshooting: E-Notifications Management”.

   Under the Results section, click Avaya Support Web Tips and Troubleshooting: E-Notifications Management.

2. Set up e-notifications.

   For detailed information, see the **How to set up your E-Notifications** procedure.

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W