Avaya Aura® Communication Manager Feature Description and Implementation

Release 10.2.x
Issue 2
April 2024

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided 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.

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, 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

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

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 to comply 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, please contact your Avaya Sales Representative.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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

Purpose

This document describes the features of Avaya Aura® Communication Manager. You can use this document to administer and troubleshoot features. For your convenience, this document presents the features in the alphabetical order.

Communication Manager features are grouped in feature sets and are administrable. Customers can control whether to enable or disable a feature.

This document is intended for anyone who wants to understand the features and functionality. The audience includes and is not limited to field technicians, business partners, solution providers, and customers.

Discontinued support for IP Server Interface (TN2312, commonly known as “IPSI”)

With Release 10.2, Communication Manager does not support the IP Server Interface (IPSI). As a result, access and functionality are removed. This means, the IPSI connected cabinets and gateways do not work with Communication Manager Release 10.2. Examples of IPSI connected cabinets and systems include G3cfs, G3csi, G3i, G3r, G3s, G3si, G3vs, G3x, G600, G650, MCC, SCC, CMC, IPSI, IP Server Interface, and IP port network.

Discontinued support also includes the TN8412, which previously paired with the TN8400 blade server. TN8412 was last supported with Communication Manager Release 5.x.

For more information, see the End of sale G650 document published on the Avaya Support website.

Organization

To ensure readability and completeness, the information for each feature is categorized into the following topics:

- Summary

- Detailed description
- Administering
- End-user procedures
- Reports
- Considerations
- Interactions
- Troubleshooting

Summary

The Summary section provides a brief description of the feature. For simple features, the Summary might be only one sentence. For more complex features, the Summary might be one or two paragraphs.

Detailed description

The Detailed Description section provides detailed information about the feature. Some features have more than one function, called capabilities.

Administering

The Administering section provides the information that you need to administer and implement the feature. This section includes the following information:

- Any prerequisite that you must complete before you administer the feature
- The screens that you use to administer the feature
- Complete administration procedures for the feature

End-user procedures

The End-user procedures section describes any procedures that might exist for a user to activate, deactivate, or otherwise modify administration of the feature, or a capability of the feature.

If a feature does not have end-user procedures, the feature description does not contain this section.

Reports

The Reports section lists the reports that provide information about the feature. If a feature does not have any reports, the feature description does not contain this section.

Considerations

The Considerations section provides any useful miscellaneous information about the operation of the feature. If a feature does not have considerations, the feature description does not contain this section.

Interactions

The Interactions section describes how the feature interacts with other features. For example, certain features must always be used in conjunction with other features. Some features cannot coexist with other features. In some cases, the normal operation of a certain feature modifies the normal operation of another feature. Some features also enhance each other, and when combined, provide improved service to the user. The features are listed in alphabetical order.

Troubleshooting

The Troubleshooting section provides a table that lists the following information:

- Known or common problems that users might experience with the operation of the feature
- Possible causes of the problems
- Actions that an administrator can take to solve the problems

If a feature does not have troubleshooting tips, the feature description does not contain this section.

Change history

Issue	Date	Summary of changes
2	April 2024	Updated the following sections: • Detailed description of send-nn calling • Screens for administering Facility and Non-Facility Associated Signaling • Service Observing with Multiple Observers
1	December 2023	Release 10.2

Chapter 2: Communication Manager overview

Communication Manager management

Communication Manager can be deployed, upgraded, or migrated using Solution Deployment Manager of System Manager.

- From Avaya Aura® Release 10.1, HP ProLiant DL360p G8 (CSR2), HP ProLiant DL360 G9 (CSR3), Dell™ PowerEdge™ R620 (CSR2), Dell™ PowerEdge™ R630 (CSR3), and Avaya Solutions Platform 120 servers are not supported.

  However, in Release 10.1, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.x, and S8300E can be upgraded to Avaya Solutions Platform S8300 R5.1.x.
- From Avaya Aura® Release 10.1, Appliance Virtualization Platform is not available for deploying or upgrading the Avaya Aura® applications. To upgrade the Avaya Aura® applications, migrate the Appliance Virtualization Platform to Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.x.

Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® applications. Solution Deployment Manager supports the operations on the customer's Virtualized Environment and the Avaya Aura® Virtualized Appliance model.

Solution Deployment Manager supports migration of Virtualized Environment-based 8.1.x or 10.1.x applications to Release 10.2.x in the customer's Virtualized Environment. For migrating to Release 10.2.x and later, you must use Solution Deployment Manager Release 10.2.x and later.

Release 7.0 and later supports a standalone version of Solution Deployment Manager, the Solution Deployment Manager client. For more information, see *Using the Solution Deployment Manager client*.

System Manager with Solution Deployment Manager runs on:

- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.
- Software-Only environment: Avaya Aura® applications are deployed on the customer-owned hardware and the operating system.

- Avaya Solutions Platform 130: Avaya Aura® applications are deployed on the Avaya provided hardware.

With Solution Deployment Manager, you can do the following in Virtualized Environment, Avaya Solutions Platform 130, and Avaya Aura® Virtualized Appliance Release 8.x or earlier models:

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.

  Note:

  When an application is configured with Out of Band Management, Solution Deployment Manager does not support upgrade for that application.

  For information about upgrading the application, see the application-specific upgrade document on the Avaya Support website.
- Download Avaya Aura® applications.
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications:
  - Communication Manager and associated devices, such as gateways, and media modules
  - Session Manager
  - Branch Session Manager
  - AVP Utilities Release 8.x
  - Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier, the ESXi host that is running on the Avaya Aura® Virtualized Appliance.
  - AE Services

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Refresh applications and associated devices and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade Avaya Aura® applications.
- Install software patch, service pack, or feature pack on Avaya Aura® applications.

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 10.2.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

Communication Manager license

Obtaining and installing the license file

The license file is an Extensible Markup Language (XML) file. The license file has the information regarding the product, major release, and license features and capacities.

You must install license files for the Communication Manager main server, but not for survivable servers. Survivable servers receive licensing information from the main server.

On System manager WebLM, if you are licensing a duplicated pair configuration, you must install the license file on both servers. The system does not synchronize the license file from active server to standby server.

A 30-day grace period applies to new installations or upgrades to Communication Manager, Collaboration Server, and Solution for Midsize Enterprise. You have 30 days from the day of installation to install a license file.

Customer Option features and the license file

Communication Manager has two categories of Customer Option features:

- Unlicensed Customer Option features that are available to all customers with the purchase of Communication Manager.
- Licensed Customer Option features that customers purchase and are controlled by the license file.

A specific feature in the Communication Manager license file may enable or map to multiple features on the Customer Options form. For example, ASAI Features (FEAT_CM_ASAI_PCKG) in the license file enables multiple ASAI-related features on the Customer Options form, including ASAI Link Core Capabilities and ASAI Link Plus Capabilities. Unlicensed features are available to all customers and are excluded from the license file.

The Communication Manager System Management Interface (SMI) provides the ability to enable or disable individual Customer Option features that have an on or off (yes or no) setting. This capability is available only for the Customer Option features to which you are entitled. Features to which you are entitled include unlicensed features plus any licensed features that are entitled based on the license file. This capability does not apply to capacity features and other types of features that do not have an on or off setting.

How Communication Manager acquires licenses from WebLM

At startup, Communication Manager contacts WebLM and requests license release, features, and capacities. WebLM responds to Communication Manager, which then uses the acquired features and capacities to set license permissions in the Communication Manager software.

Communication Manager acquires all of the feature capacity from WebLM, regardless of actual usage. For example, if the Maximum Stations (VALUE_CM_STA) feature is set to 36,000 in the license file, Communication Manager acquires capacity for all 36,000 stations regardless of the number of stations currently configured. Actual license usage can be viewed on the Customer Options form in the System Administration Terminal (SAT) interface.

Every 9 minutes, Communication Manager sends a request to WebLM to renew its license information. Because of this time interval, you may have to wait up to 9 minutes for a newly installed license file to take effect on Communication Manager.

Communication Manager license utilization

Using the License Utilization feature, you can view the license utilization on the WebLM user interface for Communication Manager, Call Center Elite, and Communication Manager Messaging. License utilization is the number of licenses actually used by a product. For example, if you have a Communication Manager license file that can support 1000 station licenses and you

add 900 stations on the Communication Manager server, the WebLM user interface displays 900 licenses.

On the WebLM server, you can view and track the license usage for all Avaya Aura® products. The standalone WebLM server, System Manager WebLM server, and WebLM OVA support the License Utilization feature.

Using the License Utilization feature, you can determine the need for buying extra licenses and identify the unused licenses of one system that you can use to increase the capacity on another system.

On the View License Capacity page of the WebLM user interface, you can view the current license utilization and peak license utilization (high water mark) for the last 7 to 30 days.

Note:

Communication Manager Release 6.3 and earlier displays all feature capacity in use, regardless of the actual utilization on the Communication Manager server.

Viewing the license capacity and utilization of the product features

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

About this task

Use this procedure to view the license capacity and license utilization of a product for which you installed a license file.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View license capacity**.

View License Capacity field descriptions

Name	Description
License File Host IDs	The host ID of the license file.

The following fields are applicable for the Solution license:

Name	Description
Active License Mode	The type of license active on WebLM. The default value is **Avaya Subscription**. The WebLM server can have Avaya Subscription and Standard (Perpetual) licenses installed. However, at a time only one license can be active. These licenses are used while switching between two modes.

Table continues…

Name	Description
License State	The status of the Avaya Subscription license. The default value is **Granted**.
Avaya Subscription License Available	The availability status of the Avaya Subscription license on WebLM. The default value is **Yes**.
Standard License Available	The availability status of the standard license on WebLM. The default value is **No**.

Licensed Features

You can view the total number of feature licenses in the license file and the current usage of those licenses.

Name	Description
Feature (License Keyword)	The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.
Expiration Date	The date on which the feature license expires.
Licensed capacity	The number of licenses for each licensed feature. WebLM fetches the number of feature licenses information from the license file. For the Solution license, the value is **Metered**.
Currently Used	The number of feature licenses that are currently in use by the licensed application. For features of type Uncounted, the column displays *Not counted*.

Acquired Licenses

The Acquired licenses table displays information about the licenses acquired by the licensed application. You can view the information in the table only if the licensed product has acquired feature licenses.

Name	Description
Feature	The feature keyword for each licensed feature that is currently acquired by a licensed application.
Acquired by	The name of the licensed application that has acquired the license.
Acquirer ID	The unique identifier of the licensed application that has acquired the license.
Count	The number of feature licenses that are currently acquired by the licensed application.

Viewing peak usage for a licensed product

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View peak usage**.

View Peak Usage field descriptions

You can view information about the usage of feature licenses of a licensed application at different time intervals.

For the Solution license, the usage fields shows the number of used license file, but not the percentage (%) of usage.

Name	Description
Feature (License Keyword)	The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.
Currently Allocated	The number of feature licenses purchased by the organization. For the Solution license, the value is **Metered**.
Usage: qty/%	The number of feature licenses for each licensed feature that a licensed application currently uses. The column also displays the percentage of usage. For example, if 50 feature licenses are available and five feature licenses are used by applications, the column displays 5/10%.
Peak Usage (today): qty	The highest number of feature licenses for each licensed feature used for the day.
Peak Usage (Last 7 days): qty/%	The highest number of feature licenses for each licensed feature used in the last seven days. For example, if the peak usage for a feature license in the past seven days was 25, and the number of available licenses during these seven days was 50, then the column displays 25/50%.
Peak Usage (Last 30 days): qty/%	The highest number of feature licenses for each licensed feature used in the past 30 days. For example, if the peak usage for a feature license in the past 30 days was 50, and the number of available licenses during these 30 days was 50, then the column displays 50/100%.
Time of Query	The date and time when the last usage query for WebLM was executed.
Status	The success or failure of the last usage query executed for the WebLM server.

Button	Description
Back	Cancels the action and returns to the previous page.

Centralized licensed products installed license files field descriptions

Name	Description
Host ID - Centralized Licensing ID	The host ID and the centralized licensing ID of the license file. The first 12 characters are the WebLM server host ID, and the last 5 characters are the centralized licensing ID. The centralized licensing ID is a unique number across multiple license files for the same product.
License Host Name	The host name of the license as defined in the license file.
Assigned To Element	The field that indicates whether a license file is associated with an element instance. The possible values are: • **Yes**: The license file is associated with an element instance. • **No**: The license file is not associated with an element instance.
Date of Installation	The date of installation of the license file.

PLDS

The Avaya Product Licensing and Delivery System PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

When you place an order for a PLDS-licensed software product such as Communication Manager, Collaboration Server, and Solution for Midsize Enterprise, the license entitlements on the order are automatically created in PLDS. Once these license entitlements are created, you receive an e-mail notification from PLDS. This e-mail notification includes a license activation code (LAC). Using LAC, you can quickly find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

Important:

You must provide the WebLM host ID to activate the license file in PLDS. The WebLM host ID is the MAC address of the server and is obtained from the WebLM Web interface.

Service Pack and Dot Release Guardian overview

Avaya Service Pack and Dot Release Guardian is patent pending technology that protects and controls the authorized use of Communication Manager Service packs and dot releases by inserting the Support End Date (SED) in the license file and comparing it to the Publication Date of the service pack or dot release. The application of service packs and dot release upgrades require Avaya support entitlements.

Using Avaya Service Pack and Dot Release Guardian technology, you can use a service pack or dot release if the Publication Date of the service pack or dot release is on or before the SED in the Communication Manager license file. Consider the following examples where the SED in the license file is 01 March 2013:

- Service Pack Guardian:
  - If the service pack Publication date is 01 March 2013 (or any earlier date), you can apply the service pack.
  - If the service pack Publication date is 02 March 2013 (or any later date), Communication Manager blocks the service pack installation.
- Dot Release Guardian:
  - If the Communication Manager software Publication Date is 01 March 2013 (or any earlier date), the Communication Manager software is allowed, and no license error displays.
  - If the Communication Manager software Publication Date is 02 March 2013 (or any later date), Communication Manager enters in license error mode with a 30-day grace period.

The SED is the expiration date for the support entitlements based on your Software Support (SSI), Software Support Plus Upgrades (SSU), Support Advantage (SA) or co-delivery support contract (for example, Joint Services Delivery (JSD) or Partner Support Services (PSS)). If you have not purchased Avaya support coverage, the SED in the license file reflects a 90-day warranty period that starts when the license entitlements are first activated.

For more information about obtaining and installing the Communication Manager licenses, see Communication Manager license section.

Communication Manager license features

A specific feature in the Communication Manager license file may enable or map to multiple features on the Customer Options form. For example, ASAI Features (FEAT_CM_ASAI_PCKG) in the license file enables multiple ASAI-related features on the Customer Options form, including ASAI Link Core Capabilities and ASAI Link Plus Capabilities. Unlicensed features are available to all customers and are excluded from the license file.

The following table summarizes the mapping of features in the Communication Manager license file to Customer Option features.

License feature	Communication Manager Customer Option features
Edition (VALUE_CM_EDITION)	`Standard` enables all unlicensed Customer Option features. `Enterprise` maps to the Multinational Locations Customer Option feature. Also enables all unlicensed Customer Option features.
Maximum Stations (VALUE_CM_STA)	Maps to multiple Customer Option features, notably Maximum Stations.

Table continues…

License feature	Communication Manager Customer Option features
Maximum Analog Stations (VALUE_CM_ANALOG)	Specifies the number of analog stations to which the customer is entitled.
Maximum Survivable Processors (VALUE_CM_SP)	Maps directly to the Maximum Survivable Processors Customer Option feature.
Maximum ESS Stations (VALUE_CM_ESS_STA)	Specifies the number of Survivable Core station licenses to which the customer is entitled.
Maximum LSP Stations (VALUE_CM_LSP_STA)	Specifies the number of Survivable Remote station licenses to which the customer is entitled.
Maximum Mobility Enabled Stations (VALUE_CM_MOBILITY)	Maps to multiple Off-PBX Telephones Customer Option features.
Maximum Video Capable IP Softphones (VALUE_CM_VC_IPSP)	Maps to the Maximum Video Capable IP Softphones Customer Option feature.
ASAI Features (FEAT_CM_ASAI_PCKG)	Maps to ASAI-related Customer Option features including ASAI Link Core Capabilities and ASAI Link Plus Capabilities.
Maximum Expanded Meet-Me Conference Ports (VALUE_CM_EMMC_PORTS)	Maps to the Maximum Number of Expanded Meet-Me Conference Ports Customer Option feature.
IP Endpoint Registration Features (for example, IP_Soft)	Map directly to Customer Option features of the same name, for example, IP_Soft.
Support End Date (VALUE_CM_SED)	Specifies the Support End Date (SED) used for Avaya Service Pack and Dot Release Guardian. If the Support End Date feature is available in the Communication Manager license file, the value is in DD-Month-YYYY format (for example, 01 June 2012). If the Support End Date feature is not available in the license file, Communication Manager does not perform the Support End Date validations. For more information, see the Service Pack and Dot Release Guardian overview section.

Viewing Support End Date

- You can view the SED for a Communication Manager server by accessing the associated WebLM server and viewing the Support End Date (VALUE_CM_SED) feature setting in the Communication Manager license file.
- You can view the SED in PLDS.
  - Select **Activation** > **View Activation Record**.
  - Search for the required record.
  - Click on the **License/Key** tab. Look for VALUE_CM_SED in the License/Key box for Communication Manager.

- The SED is contained in the VALUE_CM_SED feature.

If there is no SED value in the license file then Communication Manager does not perform the SED or Publication Date check. However, you can install the Communication Manager software or apply the service pack.

Every 9 minutes, Communication Manager sends a request to WebLM to renew its license information. Because of this time interval, you may have to wait up to 9 minutes for a newly installed license file to take effect on Communication Manager.

Viewing software Publication Date

- You can view the software publication date on the PLDS download screen on top of the download description text.
- You can view the publication date of the installed Communication Manager software on the Software Version page of Server Management Interface (SMI).
- You can use the **`swversion`** command to view the publication date of the Communication Manager software in the **Publication Date** field.
- You can view the publication date of a service pack on the System Manager.
  - If you have not downloaded the service pack, select the Download/Upload sub-menu option, and select the appropriate media to download the patch. When the service pack is successfully loaded, the details page displays the publication date.
  - If you have downloaded the service pack, select the Manage sub-menu option. Select the required service pack. The service pack details are displayed with the publication date. If the service pack **Publication Date** field is null on the patch details page, then Avaya Service Pack and Dot Release Guardian technology does not protect the service pack.

Note:

If the Communication Manager software or service pack does not contain a publication date then Avaya Service Pack and Dot Release Guardian technology does not protect the Communication Manager software and service packs.

Guardian Enforcement for Service Packs and Dot Releases

Guardian enforcement for Service Packs

Most services packs require support entitlements. Security patches do not require support entitlements. The services packs that require the support entitlement are licensed service packs. If the **License Required** field is set to yes in the ReadMe file then the service pack is the licensed service pack. When you apply a licensed service pack, the service pack publication date is checked against the SED in the Communication Manager license file.

If the service pack publication date is after the SED, Communication Manager blocks the service pack installation and System Manager displays the following error message:

```
Command Failed: Service Pack publication date is after the Support End
Date in the license file.
```

If the service pack publication date is on or before the SED, the service pack is allowed and is installed on Communication Manager.

If the **License Required** field is set to yes in the ReadMe file but there is no SED value in the license file then Communication Manager does not perform the SED or Publication Date check. However, you can apply the service pack. Later, if you want to install the license file with a SED value and the SED is before the publication date, you cannot apply the service pack. Communication Manager blocks the service pack installation. Any previously installed service pack with a publication date after the SED in the newly installed license file will not cause license errors.

If the **License Required** field is set to no in the ReadMe file, the service pack is not a licensed service pack. A service pack that does not require a license does not have a publication date and no Guardian check of the SED is performed when service pack is applied.

Guardian enforcement for Dot Releases

If you are installing a dot release with a publication date that is not allowed by the SED in the license file, Communication Manager displays a license error, enters license error mode, and starts the 30-day license grace period. The system displays the following error message in the **Administration** > **Licensing** > **License Status** screen on the System Management Interface (SMI):

```
CommunicaMgr License Mode: License Error.
System Administration Will Be Blocked in Approximately 30 days.
Contact Your Service Representative Immediately.
Software Publication Date is After the Support End Date in License File.
```

To correct the license error:

- If you have an Avaya support contract, contact Avaya or business partner to regenerate and reinstall the license file to update the SED in the license file.
- If you do not have an Avaya support contract, you can purchase support coverage.
- If you do not want to purchase an Avaya support contract to allow the dot release, you need to go back to an earlier release of Communication Manager that is consistent with your support entitlements.

If the software publication date is on or before the SED, the software is allowed and is installed on Communication Manager without a license error.

If there is no SED value in the license file then Communication Manager does not perform the SED or Publication Date check. However, you can install the Communication Manager software. Later, if you install a license file with a SED value and the SED is before the publication date, Communication Manager enters in license error mode with a 30-day grace period.

License error mode

If Communication Manager detects an error with the licensing, for example, license file is not installed, feature usage exceeds license capacity, or software publication date is after the SED in the license file, the Communication Manager server enters in license error mode, raises a

major alarm, and starts a 30-day license grace period. During the 30-day license grace period, Communication Manager provides full normal operations.

- If the license grace period expires before the license error is resolved, Communication Manager enters no license mode. In no license mode, Communication Manager continues to provide call processing. However, you cannot administer the system.
- If the license error is resolved either before or after expiration of the 30-day grace period, Communication Manager returns to license normal mode.

Communication Manager license features

A specific feature in the Communication Manager license file may enable or map to multiple features on the Customer Options form. For example, ASAI Features (FEAT_CM_ASAI_PCKG) in the license file enables multiple ASAI-related features on the Customer Options form, including ASAI Link Core Capabilities and ASAI Link Plus Capabilities. Unlicensed features are available to all customers and are excluded from the license file.

The following table summarizes the mapping of features in the Communication Manager license file to Customer Option features.

License feature	Communication Manager Customer Option features
Edition (VALUE_CM_EDITION)	`Standard` enables all unlicensed Customer Option features. `Enterprise` maps to the Multinational Locations Customer Option feature. Also enables all unlicensed Customer Option features.
Maximum Stations (VALUE_CM_STA)	Maps to multiple Customer Option features, notably Maximum Stations.
Maximum Analog Stations (VALUE_CM_ANALOG)	Specifies the number of analog stations to which the customer is entitled.
Maximum Survivable Processors (VALUE_CM_SP)	Maps directly to the Maximum Survivable Processors Customer Option feature.
Maximum ESS Stations (VALUE_CM_ESS_STA)	Specifies the number of Survivable Core station licenses to which the customer is entitled.
Maximum LSP Stations (VALUE_CM_LSP_STA)	Specifies the number of Survivable Remote station licenses to which the customer is entitled.
Maximum Mobility Enabled Stations (VALUE_CM_MOBILITY)	Maps to multiple Off-PBX Telephones Customer Option features.
Maximum Video Capable IP Softphones (VALUE_CM_VC_IPSP)	Maps to the Maximum Video Capable IP Softphones Customer Option feature.
ASAI Features (FEAT_CM_ASAI_PCKG)	Maps to ASAI-related Customer Option features including ASAI Link Core Capabilities and ASAI Link Plus Capabilities.

Table continues…

License feature	Communication Manager Customer Option features
Maximum Expanded Meet-Me Conference Ports (VALUE_CM_EMMC_PORTS)	Maps to the Maximum Number of Expanded Meet-Me Conference Ports Customer Option feature.
IP Endpoint Registration Features (for example, IP_Soft)	Map directly to Customer Option features of the same name, for example, IP_Soft.
Support End Date (VALUE_CM_SED)	Specifies the Support End Date (SED) used for Avaya Service Pack and Dot Release Guardian. If the Support End Date feature is available in the Communication Manager license file, the value is in DD-Month-YYYY format (for example, 01 June 2012). If the Support End Date feature is not available in the license file, Communication Manager does not perform the Support End Date validations. For more information, see the Service Pack and Dot Release Guardian overview section.

Type 3 License Allocation Algorithm

Communication Manager implements Type 3 License Allocation Algorithm during registration and unregistration. Based on the content of the license file, Type 3 License Allocation Algorithm provides multiple Type 3 feature entries for the same product ID with different releases. An available license can be used for a registered endpoint if the release number of the license is identical to the release number of the registered endpoint or a later version of the registered endpoint.

Communication Manager uses Type 3 License Allocation Algorithm to:

- Check the available capacity of the license for the same release and product ID of the registering endpoint, and uses the license based on the available capacity
- Search for available licenses of incremental releases for the product ID if adequate capacity is unavailable
- Search for any release of an available license if licenses with specific releases for the product ID are unavailable
- Release the available license at the time of unregistration

Type 3 License Allocation Algorithm is used to register licenses of multiple releases with endpoints of multiple releases. Type 3 License Allocation Algorithm provides the benefit of optimum usage of licenses and easy upgrade of the licenses for endpoints.

Type 3 License Allocation Algorithm uses the lowest-priced license for registration and releases the highest-priced license at the time of unregistration.

Call Center license features

The following table summarizes the mapping of features in the Call Center license file to Customer Option features.

License feature	Call Center Customer Option features
Maximum Elite Agents (VALUE_CC_ELITE)	Maps to multiple Customer Option features, most notably Logged-In ACD Agents.
Maximum Advocate Agents (VALUE_CC_ADVOCATE)	Maps to multiple Customer Option features, most notably Logged-In Advocate Agents.
Proprietary (FEAT_CC_PROPRIETARY)	Maps directly to the Proprietary Customer Option feature (renamed from Agent States in Communication Manager 6.0).
Call Center IP Endpoint Registration Features (for example, IP_Agent)	Maps directly to Customer Option features of the same name, for example, IP_Agent.

Feature server

A feature server provides Communication Manager features to the SIP endpoints registered with Session Manager. The feature server uses the half-call model of IP Multimedia Subsystem (IMS).

The feature server supports full application sequencing.

The feature server has the following limitations:

- The feature server does not support routing of PSTN calls directly to ISDN trunks for IMS users. You must administer the dial plan to route all PSTN calls to Session Manager over the IMS trunk group.
- The feature server does not support traditional endpoints, such as DCP, H.323, ISDN, and analog.
- The feature server does not support call reconstruction.

Half-call model

The half-call model processes a call request in two phases:

- Origination: The feature server applies services to the originator of the call.
- Termination: The feature server applies services to the recipient of the call.

The origination phase and the termination phase are separate operations that different feature servers perform.

The half-call model supports full application sequencing. The number of originating sequenced applications can be different from the number of terminating sequenced applications.

ASAI support for feature server

ASAI supports the half-call model of the Communication Manager feature server. With this support, Communication Manager can use the legacy Computer Telephony Integration (CTI) applications and the Avaya Breeze® platform applications.

ASAI processes half calls similarly to full calls. ASAI maps the Communication Manager caller IDs of multiple half calls to a unique virtual ASAI caller ID to identify the full call in ASAI messages. When CTI adjuncts use this virtual ASAI caller ID in messages, ASAI maps the caller ID with the Communication Manager caller IDs for call processing. ASAI generates the same call processing messages for the full-call model in the feature server as the evolution server.

Support for Channel Type identification over ASAI to CTI application

Communication Manager supports channel type identification over ASAI to a CTI application from 7.1.1 onwards. For incoming SIP trunk calls, Communication Manager Release 7.1.1 and later 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 11.

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

Evolution server

An evolution server is similar to the traditional Communication Manager server. The evolution server provides Communication Manager features to both SIP and non-SIP endpoints. The evolution server uses the full-call model. The evolution server connects to Session Manager through a non-IMS Signaling group. Session Manager handles call routing for SIP endpoints and enables SIP endpoints to communicate with all other endpoints that are connected to the evolution server.

If you configure Communication Manager as an evolution server:

- H.323, digital, and analog endpoints register with Communication Manager.
- SIP endpoints register with Session Manager.
- All endpoints receive service from Communication Manager.

The evolution server supports a limited form of application sequencing.

Full-call model

The full-call model processes a call request in a single step and performs the origination and the termination phase without a break. The traditional Communication Manager server follows the full-call model.

Application sequencing works only when all servers support the half-call model. Therefore, do not provision other sequenced applications with the evolution server.

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.

Special application activation process

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

Some of the special features should not be set without the right configurations, and some features should not be set together at the same time. Otherwise, the feature may not operate as expected, the system performance could be affected or both. To avoid users from setting those features accidentally, Communication Manager has identified those features and marked them as restricted. To activate the restricted features, customers must go to http://support.avaya.com.

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

Chapter 3: AAA Services

Using the Authentication, Authorization and Accounting (AAA) services feature, you can store and maintain administrator account (login) information on a central server.

Note:

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

Detailed description of AAA Services

To interact with Avaya Aura® Communication Manager, AAA services use the Authentication Module (PAM and Linux) and Name Service Switch (NSS) within Linux. These mechanisms are supported on Linux-based Communication Manager servers.

External AAA support is a Linux feature that is separate from Communication Manager, is not controlled by a license file, and is freely available to the customer. Customers can use the same authentication for Communication Manager as is used by other servers on their network.

PAM is an application programming interface that provides great flexibility to process administrator's account.

Name Service Switch (NSS) is a Linux facility that provides the source of authorization information. The source can be local files on the Communication Manager server.

Supported security configurations

The following security configurations are supported on Communication Manager:

Local host accounts

- All authentication, authorization, and accounting information is maintained on the same server to which the user is attempting access. For Communication Manager, this is the Communication Manager server.
- Use the files `/etc/passwd`, `/etc/shadow`, and `/etc/group` among others.

RSA SecurID based accounts

- Require a parallel local host account for authorization information.
- Can be used directly from the Communication Manager server, when a license is purchased from the vendor and software is installed on the Communication Manager server.

Secure Computing SafeWord accounts

- Require a parallel host account for authorization information.
- Can be used directly from the Communication Manager server, when a license is purchased from the vendor and software is installed on the Communication Manager server.

External AAA servers configuration

The Communication Manager default configuration does not contain an entry for an external AAA server. All accounts are authenticated on the local host.

To activate use of an external AAA server, the `/etc/pam.d/mv-auth` file must be edited to incorporate the appropriate line for the server being used, and the additional configuration files edited corresponding to the needs of the AAA service. Activation of an external AAA service will be accomplished by the customer and not by Avaya Services. The customer provides and owns the AAA server on their network and they alone have the data that is necessary to set up the client on the Communication Manager server.

For information regarding configuring AAA Servers, see:

- *Communication Manager Administrator Logins* White Paper on http://www.avaya.com/support
- http://www.kernel.org/pub

  This Web site contains PAM documentation such as the System Administrators' Guide.

Also see documentation for:

- Individual PAM modules
- Applications running on external servers

User authentication with AAA Services

Communication Manager login authentication takes place in Linux PAM modules, and the system configuration determines how user authentication takes place. For example, if the user's account is EASG protected, the Linux PAM module will issue the appropriate challenge. If a token device is used such as *SecurID* from RSA Security, the user may be prompted for a pin plus the token's displayed value.

User profiles with AAA Services

Profiles govern access to the Communication Manager SAT and to the Communication Manager System Management Interface (SMI). A profile consists of a numeric identifier and that profile's access permissions. Administration for SAT profiles and web profiles are separate processes.

- Communication Manager SAT profiles define access to Communication Manager SAT screens. SAT profile data is maintained within Communication Manager.
- Communication Manager web profiles define access to Web pages in the web interface. Web profile data is maintained in a Linux file.

- SAT profile objects (SAT screens) and web profile objects (Web pages) have no objects in common.
- A profile is identified by a number 0-69, which corresponds to a Linux group. Both Communication Manager and the web interface dedicate fixed permissions to profiles 0-19, which may not be deleted or modified.
- When a profile is created, the profile is assigned to a Linux group whose number is Communication Manager_PROFILE_BASE or greater. Communication Manager_PROFILE_BASE defaults to 10,000 for both Communication Manager and the Web. The value can be changed through the Web pages.
- Profile numbers are based on the login's Linux group number, minus the Communication Manager_PROFILE_BASE. For example, user **dadmin** belongs to Linux group 10,002. The profile number for **dadmin** is 2 (10002 minus 10000).
- When a Linux group is assigned to a login, the login is assigned the profile associated with that Linux group. For example, when Linux group 10,002 is assigned to the **dadmin** login, **dadmin** is automatically assigned user profile 2.
- Communication Manager maintains up to 70 profiles.
- A login may be assigned exactly zero or one user profile. A login may not be assigned to more than one user profile. If a login is not assigned group membership in the range 10,000 to 10,069, that login will have no access to the SAT or the server Web pages. Multiple logins may be assigned to the same profile. The starting value of 10,000 may be changed through the Web Access Mask page.

To access Communication Manager functions according to job functions, create and modify profiles. Examples of such profiles are:

- Security Auditor profile, with read-only access to logs and audit files.
- Security profile, with read/write access to create other administrator logins, create and modify profiles.
- Telephony Application Administrator profile, with read/write access to application configuration, such as trunks.
- Backup administrator profile, with the ability to perform only backups.
- Telephone Provisioning profile, with ability to add/change/delete a certain range of telephone extensions.
- ACD Administrator profile, with the ability to modify call center vectors.
- Checker profiles, with read-only access, able to only view certain changes.

User profiles for SAT form access with AAA Services

In Communication Manager, the profile specifies which SAT screens may be accessed by the user assigned the profile. The profile further defines the type of access to each screen. A user with appropriate permissions can change the SAT profile permissions by editing the User Profile (**`change user-profile`**) form.

The SAT User Profile form specifies access for every Communication Manager SAT form (object). The list of Communication Manager objects is maintained in Communication Manager. The SAT

profile form lists all the possible SAT screens in the software regardless of whether the associated feature is enabled, disabled, licensed or not licensed.

On the User Profile form, SAT screens are grouped in categories. SAT screen categories:

- Exist only for the organization of the User Profile form
- Lets the user quickly set permissions for a group or groups of screens for a profile
- Provides a summary of the groups of screens that can be accessed by the profile

AAA Services SAT profiles

SAT profiles control access to SAT screens based on the command object (SAT screen).

Seventy user-profiles exist in Communication Manager, numbered 0-69, which correspond to a Linux group.

- Profiles 0-19 are dedicated. Profiles 0-17 cannot be edited, copied, viewed, nor removed. Profiles 18 and 19 may be assigned to any customer login.
- Profile numbers 20-69 are available for customer use for customized profiles.

Table 1: Communication Manager User Profiles

Profile	Profile name	Permissions/access	Notes
0	services super-user	Equivalent to the former SAT **init** login. Has all permissions possible with no restrictions.	Cannot be edited, copied, viewed, or removed. Restricted Requires a second user authentication by Communication Manager.
1	services manager	Equivalent to the former SAT **inads** login	Cannot be edited, copied, viewed, or removed. Requires a second user authentication by Communication Manager.
2	business partner	Equivalent to the former SAT **dadmin** login	Cannot be edited, copied, viewed, or removed. Must be enabled in the license file. The **dadmin** login can create one login that has craft login permissions and a name other than craft. The second craft login uses Profile 3 and can login without a second challenge.

Table continues…

Profile	Profile name	Permissions/access	Notes
3	services	Equivalent to the former SAT **craft** login	Cannot be edited, copied, viewed, or removed. Requires a second user authentication by Communication Manager.
4-15		Reserved for future use by Avaya.	Cannot be edited, copied, viewed, or removed.
16	call center manager	Equivalent to the former SAT MIS login (@MIS) CMS/CCR access	Cannot be edited, copied, viewed, or removed. Assign CMS/CCR logins through the MIS application.
17	snmp	SNMP agent access	Cannot be edited, copied, viewed, or removed.
18	customer super-user	Equivalent to the former SAT default customer super-user login	Cannot be edited or removed.
19	customer non-super user	Equivalent to the former SAT default non-super-user customer login	This profile is used during upgrades only. It has no SAT permissions. Cannot be edited or removed.
20-69		Available for customer modification	

AAA Services extended profiles

Extended profiles provide additional access control for vector and station forms.

As an example of increased access control through extended profiles, you can use an extended profile to grant access to a specific set of vectors. For example, a user profile has read-only (`r-`) access to the vector form in the standard profile. The extended profile grants access to vector 3 only. The user is able to display vector 3 and is able to list vectors. A user with these restrictions can see (list) all vectors, but can read the detail parameters only for vector 3.

User profiles for Communication Manager server Web page access

On the Communication Manager Web server interface, the Web Access Mask page specifies which Communication Manager server Web pages a user may access. The Web profile is sometimes called the Web Access Mask. The Web profile defines the type of access to each Web page. You can view only those Web pages permitted by the Web profile when you access the Web interface.

The Web Access Mask Web page specifies read or read/write access for every Web page.

Using Communication Manager Web pages, you can access those functions that are normally restricted to the root login. Logins that are members of the **susers** Linux group may have full

access to the Web pages. Logins that are members of the **users** Linux group may have only limited access to the Web pages.

The Web profile has an identification number between 0 to 69. This number corresponds to a Linux group.

- The Web profile numbers, 0 to 19, correspond to the fixed profiles, 0 to 19, in Communication Manager. Profile numbers 0 to 3, 18, and 19 are built into Communication Manager and cannot be edited.
- Profile numbers 0 to 3 and 18 have access to all Web pages, as members of the Linux group **susers**.
- Profile number 19 has access to a subset of Web pages as a member of the **users** Linux group.
- Profile numbers 4 to 17 are reserved for future use.
- Profile numbers 20 to 69 are available for customer use for customized profiles.

Logins that are members of the **susers** Linux group and a member of the profile group prof18, corresponding to profile 18, have access to all the possible Web pages.

Logins that are members of the **users** Linux group and a member of the profile group prof19, corresponding to profile 19, are redirected to a subset of the Web pages.

When adding a user profile, Avaya recommends copying profile 18 for **susers** (customer super-user access) or profile 19 for **users** (customer non-super-user access) depending on the basic Communication Manager web access required, and reducing the permissions as required.

The figure on page 75 shows the process used to manage Communication Manager web profiles. The user's profile is identified by subtracting the Profile offset base (Communication Manager_PROFILE_BASE) from the user's Linux group number.

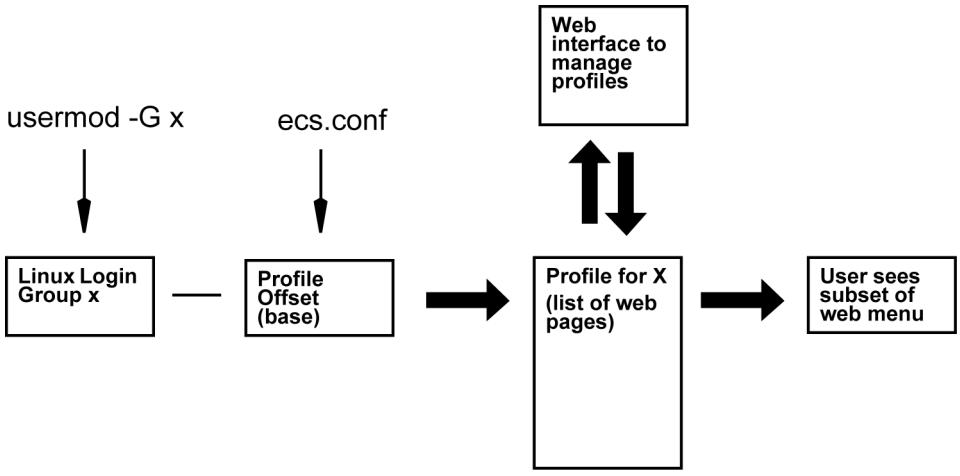


Figure 1: Web user profile overview

AAA Services Profile access to restricted objects

Communication Manager objects (commands) accessible by profile numbers 0, 1, 2, 3 are logins **init**, **inads**, **dadmin** and **craft**. Profile numbers 18 and 19 (customer super-user and

non-superuser) and customer created profile numbers 20 to 69 never have access to these commands.

Using Communication Manager objects, you can have different access for Avaya services logins and customer logins. For example, a services login might be able to execute a change or display for a certain object while customer logins can execute only a display for the same object.

The most restricted objects are accessible only by profile numbers 0, 1, and 2 (logins **init**, **inads**, and **dadmin**). These objects are listed in the table on page 76.

Table 2: Profile access to restricted objects

Object	Profile 0 init	Profile 1 inads	Profile 2 dadmin
angel (0,1)	x	x	
cumaudits	X	X	X
enable save-translations	X	X	
enable craft2 disable craft2	X	X	X
fw-log	X	X	X
hardware-group	X	X	X
internal-data	X	X	X
MO	X	X	X
MO-all	X	X	X
no-lic-mode	X	X	X
options	X	X	X
peakaudits	X	X	X
software display software errors	X	X	X
tcm	X	X	

AAA Services user accounts

You can create user accounts that have access to subset of administration functionality intended for the job or role associated with the user.

An administrator account consists of a login that belongs to either Linux group **susers**, or **users** and no profile group, or exactly one profile group for permission to access the Communication Manager SAT and System Management Interface. There are other accounts that need to be in different groups, such as remote access accounts that need to be in the Linux group **remote**. User accounts can be created and stored locally on Communication Manager, or on an external central AAA server.

When Communication Manager software is first installed, only local host accounts are configured. The Linux PAM files on Communication Manager must be edited to incorporate support for any other type of account.

See the *Communication Manager Administrator Logins* White Paper on http://www.avaya.com/support for information on editing PAM files and AAA Server configuration.

AAA Services external accounts

External accounts are accounts where authentication takes place outside of Communication Manager. Login and security information is stored in a central location.

At least one local host account should be present in all servers so that access is possible even if external AAA servers are inaccessible.

AAA Services local host accounts

A local host account is an administrative account in which all information is maintained on the same server where the login occurs.

These accounts are authenticated by PAM authentication software that resides on Communication Manager, without interacting with other AAA Services.

Fixed profiles exist for the following logins: **init**, **inads**, **craft**, **dadmin** customer superuser and non-superuser, and profiles for SNMP and CMS access.

Additional local user accounts can be created. A web interface and CLI commands (CMuser commands) exist for adding or removing additional local user accounts.

Local host accounts can be used at the same time as any of the external AAA Services.

Administrative logins with AAA Services

Use administrative logins to administer the Communication Manager server by using the SAT interface, or System Management Interface.

The access provided to an administrative login is controlled by whether or not the login is assigned a shell and the user profile assigned to the login. See User profiles for Communication Manager server Web page access on page 74. To assign a user profile to an administrative login, assign an additional group to the login by selecting **Security** > **Administrator Accounts** in Server Administration Interface.

Administrative logins cannot be used to establish a PPP session nor to acquire CDR records.

Avaya services logins with AAA Services

Profiles for Avaya services logins **init**, **inads**, **craft** are programmed into Communication Manager.

Table 3: Avaya services logins and profiles

Login	Profile
init	0
inads	1
craft	3

Services logins (**init**, **inads**, and **craft**) are EASG authenticated accounts and require two logins when used to access the Communication Manager SAT. PAM requires the first login, and Communication Manager software requires the second login. There is no prompt for the user name in the second login.

CDR logins with AAA Services

Use a **CDR** login to retrieve CDR records stored on the Communication Manager server. When creating a **CDR** login, in Server Administration Interface, click **Security** > **Administrator Accounts** and then enter `CDR_User` as the login group and leave the additional groups field blank.

BusinessPartner login: dadmin with AAA Services

The user login **dadmin** corresponds with Profile 2, BusinessPartner. Enable the **dadmin** login field in the license file required to access the Communication Manager SAT interface.

Using the **dadmin** login, you can create one login that has craft login permissions and a name other than craft. The second craft login corresponds with Profile 3. You can log in as craft without the system prompting for a second login.

A personal identification number (PIN) is added to **dadmin** and **craft2** logins (second craft login) for an additional security for BusinessPartner logins. This PIN is also used to reset a user password if an external authentication server is used. As an administrator, you must enter a PIN upon initial SAT access to the **dadmin** and the **craft2** logins. In subsequent accesses, first you must access SAT with **dadmin** or **craft2** logins to be in control of the PIN.

Remote logins: remote with AAA Services

Use a **remote** login to establish a PPP session with the Communication Manager server through its modem interface. When creating a **remote** login on the System Management Interface, specify a **remote** login Login ID (name), but you cannot specify group membership or select a shell. A **remote** login is created in the **remote** Linux group.

Remote logins cannot be used to access a shell, a SAT, CDR records, or the Communication Manager System Management Interface. **Remote** logins cannot be changed to an administrative or CDR login; instead, delete the remote login and create a new administrative or CDR login.

Linux groups with AAA Services

User authorization for administrator logins for Communication Manager servers is specified and controlled by assignment to Linux groups. Each login must be assigned to at least one primary

Linux group **susers** or **users** plus one or no profile group, **prof18** to **prof69**. When a login is assigned to a Linux group, the user gains access based on the permissions for the group.

Assign logins to **susers** carefully. **suser** logins have privileged access to the server including the ability to modify many critical system files, and the ability to add, remove and modify system logins.

For login access based on user profiles, create new Linux groups in the range 10,020 - 10,069. Avaya recommends the group name be in the form **prof-*nn*** where *nn* is the group number. For example, create **prof22** for the Linux group corresponding to access profile 22. **Prof22** is assigned the group number 10,022. With this naming convention, if a system's existing Linux groups require that the base value (10,000) be changed through the Web Access Mask page, that page will search for groups named in this manner and convert the group numbers to the new base. Groups not named in this manner will not be converted.

Table 4: Linux Groups and access permissions

Linux group name	Linux group number	Communication Manager login	Web access	SAT command access
users	100 (users)	--	Limited Menu	Limited Access
susers	555 (susers)	--	Full Menu	Full Access
remote	888 (remote)	--	PPP access to the Communication Manager platform Logins assigned to the **remote** group should not be members of any other group.	
voice	102		Access to the coresident voice mail product on the Communication Manager platform	
prof0 to **prof69**	10,000 - 10,069	Communication Manager profile 0 - 69	Web profile (access mask) 0-69, applied against limited or full Web page menu	--

Pre-release 4.0 Communication Manager software sets Linux groups as shown in the table on page 79. Communication Manager Release 4.0 and later application software is independent of these fixed assignments, but the web interface requires the assignments.

Table 5: Existing Login Group Numbers

Linux Login Group		Communication Manager Service Level	Communication Manager Login Type	Avaya Logins
Number	**Name**			
100	users	non-super-user	customer	--
102	voice			tsc
123	audix			--

Table continues…

Linux Login Group		Communication Manager	Communication Manager	Avaya Logins
Number	Name	Service Level	Login Type	
555	susers	super-user	customer/services	init, inads, craft, dadmin
888	remote	remote	customer	rasaccess

Upgrades from a release that does not support profiles

After an upgrade from a release that does not support profiles to a release that does support profiles, logins and their SAT and web access permissions are the same as before the upgrade.

Translations are processed into release 4.x and later as follows:

- A **remote** login is created in the **remote** Linux group if one does not already exist.
- A customer non-super-user login without a change in permissions is associated with profile 19.
- A customer non-super-user login with a change in permissions is associated with the next available unused profile, and the profile is configured to match SAT forms from the prior release.

  A login is created in Linux with membership in the **users** group plus group **PROF19** or the new profile number, as appropriate.
- A customer super-user login without a change in permissions is associated with profile 18.
- A customer super-user login with a change in permissions is associated with the next available unused profile, and the profile is configured to match SAT forms from the prior release.

  The login is created in Linux with membership in the **susers** group plus group **PROF18** or the new profile number, as appropriate.
- A parallel web access profile is created for each new SAT profile created during the upgrade. The web profile configuration is copied from the web profile 18 for logins in the **susers** Linux group, and from profile 19 for logins in the **users** Linux group.

Upgrades from a release that supports profiles

SAT and Web Profile information is preserved on upgrades from a release that supports profiles. Each profile that exists in the prior release also exists in the new release.

For profiles 0-19, the new release provides permissions.

For profiles 20-69 that exist in the prior release, permissions after the upgrade are set as follows:

- SAT and Web objects that appear in both releases retain their permissions.
- SAT and Web objects that appear in the prior release but not in the new release do not appear in profiles in the new release.

- Access permissions for objects that only appear in the new release are set to applicable default permission settings. In most cases, if on the User Profile screen, the Page 1 category field is enabled (y), the object is set to:
  - **w** - for an object that supports add, change, and remove actions
  - **r** - for an object that supports display and list actions
  - **-** - for an object that does not have the applicable feature license activated

Third-party AAA Services software can be reinstalled after a Communication Manager server upgrade. See the *Communication Manager Administrator Logins* White Paper on http://www.avaya.com/support for more information.

Backup and restore with AAA Services

When restoring security information from a release that supports profiles, profile information is preserved from the backup.

When restoring security information from a release that does not support profiles, the backup program run by the backup/restore Web pages:

- restores the Avaya Authentication file
- restores the files `/etc/passwd`, `/etc/shadow`, `/etc/group`, which contain user account information for users in **users** and **susers** Linux groups
- adds the needed accounts to Linux as required, including default Communication Manager profiles
- sets up default profiles and their administrator accounts provided by the new Communication Manager installation
- adds the needed accounts to Linux as required

Backup and file sync for web access profiles

A Communication Manager backup includes the web profile file(s) in the security data set. SAT profiles are backed up as part of Communication Manager translations. Web profiles are file synchronized only when manually requested from the Web Access Mask page.

File synchronization distributes the following files to all the servers in the configuration:

- `/etc/passwd`
- `/etc/shadow`
- `/etc/group`

The login account or Linux group that you have created appears on all servers in the configuration after file synchronization. The user's home directory (`/var/home/user-ID`) is created as necessary. However, the content of the user's home directory is not file synchronized.

Initiate Web access mask file synchronization from the Communication Manager **Web page Security** > **Web Access Mask**.

AAA Services administration

The following tasks are part of the administration process for AAA Services.

- Account management using Communication Manager Web pages
- Profile management using the Communication Manager SAT
- Passwords and Access Security Gateway management
- Communication Manager web access profiles administration
- User profiles for Communication Manager SAT access administration

Related links

Account management using Communication Manager Web pages on page 83
Profile management using the Communication Manager SAT on page 88
Communication Manager web access profiles administration on page 88
User profiles for Communication Manager SAT access administration on page 90

Screens for administering AAA Services

Screen name	Purpose
Server Administration Interface: **Security** > **Administrator Accounts**	Adding an administrator account (login) on page 83 Changing a login on page 85 Removing a login on page 85 Locking a login on page 86 Adding a login group on page 87 Removing a login group on page 87 Adding web access profiles on page 88 Changing web profiles on page 89 Duplicating web profiles on page 89 Deleting web profiles on page 90 Changing The profile base through the Web on page 90 Displaying the profile base on Server Administration Interface on page 90

Table continues…

Screen name	Purpose
User Profile (SAT Screen)	Adding a user profile for using The SAT on page 88 Adding SAT profiles on page 90 Adding extended profiles on page 91 Duplicating SAT profiles on page 92 Deleting SAT user profiles on page 92 Deleting extended profile on page 92 Displaying the profile base at SAT on page 92 Exporting SAT profiles on page 92 Importing SAT profiles on page 93

Account management using Communication Manager Web pages

Using Administrator Accounts Web pages, you can add, change, lock, or remove local administrator logins and login groups on this server. Logins that are authenticated in an external server cannot be managed from this page.

Logins that are member of the **susers** Linux group can have full access to all the Web pages. Logins that are members of the **users** Linux group have limited access to Communication Manager Web pages. Using **Security** > **Web Access Mask** Web page, you can further restrict individual logins in the **susers** and **users** Linux groups based on membership in a secondary (profile) Linux group.

Avaya recommends that you use the Communication Manager web interface to manage administrator accounts.

Adding an administrator account

About this task

When you deploy the Communication Manager OVA using the vSphere client, perform the following procedure after the OVA deployment.

Note:

When you deploy the Communication Manager OVA using vCenter or System Manager Solution Deployment Manager, the system prompts you to specify the login name and password for the Communication Manager privileged administrator account during the deployment.

Procedure

1. Log in to Communication Manager System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the left navigation pane, click **Security** > **Administrator Accounts**.

4. Select **Add Login**.
5. Select the **Privileged Administrator** login for a member of the SUSERS group.

   You can also add the following types of login:

   - **Unprivileged Administrator**: This login is for a member of the USERS group.
   - **SAT Access Only**: This login has access only to the Communication Manager System Administration Terminal (SAT) interface.
   - **Web Access Only**: This login has access only to the server webpage.
   - **CDR Access Only**: This login has access only to the survivable CDR feature.
   - **Business Partner Login (dadmin)**: This login is for primary business partners.
   - **Business Partner Craft Login**: This login is for profile 3 users.
   - **Custom Login**: This login is for administrators with login parameters that you can customize. You can create a new user profile and later add users with this new profile.
6. Click **Submit**.

   The system displays the Administrator Login - Add Login screen.
7. In the **Login name** field, enter the administrator login name.

   The login name:

   - Can have alphanumeric characters.
   - Can have an underscore (_).
   - Cannot have all numberic characters (0 - 9).
   - Cannot have more than 31 characters.
8. In the **Primary group** field, enter **susers** for a privileged login.
9. In the **Additional group (profile)** field, add an access profile.

   The system automatically populates the values in the **Linux shell** and the **Home directory** fields.
10. To set lock parameters for the login, select the **Lock this account** check box.

    Note:

    If you set the lock parameters, the user cannot log in to the system.
11. In the **SAT Limit** field, enter the limit for the concurrent SAT sessions.

    Note:

    You can assign up to five concurrent sessions or retain the default value none. If you retain the default value, the restriction on the number of concurrent sessions does not apply to the login. However, the restriction applies to the system.
12. To assign an expiry date to the login, in the **Date on which account is disabled** field, enter the date in the yyyy-mm-dd format.

13. In the **Enter password or key** field, enter the password for the login.
14. In the **Re-enter password or key** field, reenter the same password.
15. **(Optional)** To change the password after the first login, in the **Force password/key change on next login** field, select yes.
16. Click **Submit**.

Changing an administrator account

Procedure

1. Log on to Communication Manager System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the left navigation pane, in the **Security** section, click **Administrator Accounts**.
4. Select **Change Login**.
5. From the drop-down list, select the login that you want to modify.
6. Click **Submit**.
7. In the Administrator Logins -- Change Login page, make the required changes to the fields.

   In the **SAT Limit** field, enter the limit for the concurrent SAT sessions.

   Note:

   You can assign up to five concurrent sessions or retain the default value none. If you retain the default value, the restriction on the number of concurrent sessions does not apply to the login. However, the restriction applies to the system.
8. Click **Submit**.

Removing an administrator account

Procedure

1. Log on to Communication Manager System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the left navigation pane, in the **Security** section, click **Administrator Accounts**.
4. Select **Remove Login**.
5. Select the name of the login you want to delete.
6. Click **Submit**.

   Note:

   When you add the account again, specify the SAT limit.

Viewing local host logins

About this task

This procedure provides steps to view the details of administrator accounts.

Procedure

1. Log on to Communication Manager System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. On the left navigation pane, in the **Security** section, click **Login Reports**.
4. Select **List Local Host Logins**.
5. Click **Continue**.
6. The system displays the Login Reports-- List Local Host Logins screen with information about the following parameters:
   - Name
   - Type
   - Group
   - Profile
   - Shell
   - Locked (Shadow, PAM)
   - Expires (Passwd, Account)
   - System Login
   - SAT Limit

Locking a login

About this task

Lock a login to deny access to the account. For example, lock the login when you want to deny access but don’t want to remove the account completely, such as for a person who has left the company.

Procedure

1. On Communication Manager Server Administration Interface, click **Security** > **Administrator Accounts**.
2. Enter a name or number in the box labeled **Enter Login ID or Group Name**.
3. Click **Lock/Unlock login**.
4. Click **Submit**.

Adding a login group

Procedure

1. On Communication Manager Server Administration Interface, click **Security** > **Administrator Accounts**.
2. Enter a name or number in the box labeled **Enter Login ID or Group Name**.
3. Click **Add Login Group**.
4. Click **Submit**.
5. On the Add Login Group page, enter the number of the Login Group.
6. Click **Add**.

Removing a login group

About this task

Do not remove a login group that has any login assigned to the group.

Procedure

1. On Communication Manager Server Administration Interface, click **Security** > **Administrator Accounts**.
2. Enter a name or number in the box labeled **Enter Login ID or Group Name**.
3. Click **Remove Login Group**.
4. Click **Delete**.

Modifying the maximum number of simultaneous logins for a user

About this task

From Release 7.1, Communication Manager allows default five simultaneous connections for a user. Use the following procedure to change the maximum number of simultaneous logins for the user.

Procedure

1. Log on to the Communication Manager System Management interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the navigation pane, click **Security** > **Login Account Policy**.
4. In the **Login Limits** section, in the **Maximum Number of Simultaneous logins for a user** field, enter the new value.

   Note:

   If a user is configuring *n* connections in System Manager for Connection Pooling, you must set the value to *n+1*.

5. Click **Submit**.

Profile management using the Communication Manager SAT

Adding a user profile for using SAT

Procedure

1. At SAT, enter `add user-profile`.
2. Edit the profile to restrict or give permission to the user as required.

Enabling a second craft login at SAT

Before you begin

Enable **dadmin** in the license file.

- Using **dadmin** you can enable only one second **craft** login.
- The first **craft** login must already exist.
- Create the login using the Communication Manager **Security** > **Administrator Accounts** server Web pages or in an external AAA server, if the login does not exists.

About this task

To enable a second **craft** login associated to user-profile 3 (create the permissions for the second **craft** login):

Procedure

1. Login to the Communication Manager server using the **dadmin** login.
2. Enter **`sat`** to invoke Communication Manager
3. Enter **`enable craft2`** *xyz*, where *xyz* is the unique name for the login. This login has the same permissions as the **craft** login and uses Profile 3.

Communication Manager web access profiles administration

Adding Web access profiles

About this task

When adding a Web profile, Avaya recommends copying Profile 18 for **susers** (customer super-user access) or Profile 19 for **users** (customer non-super-user access) depending on the basic Communication Manager access required, and reducing the access permissions as required.

Recommended procedure for adding Web profiles

About this task

Examine the Web menu for profiles 18 and 19. If the menu for profile 19 contains all the Web pages a user needs, copy profile 19 to create the new profile. If the user needs access to pages that are absent from profile 19, copy profile 18 to create a new profile. Edit the new profile to

remove access for Web pages the user does not need. Access to Web pages in profile 18 requires the login to be in the **susers** group.

Procedure

1. On Communication Manager Server Administration Interface, click **Security** > **Web Access Mask**.
2. On the Web Access Mask page, click **Add** button.
3. Enter the new profile number (20-69) in the box labeled **Enter new Access Mask Number**.
4. Select **Create by Copying values from Access Mask number**.
5. Enter `18` to copy super-user permissions, or `19` to copy non-super-user permissions.

   You may also copy any other existing profile and its unique permissions to create a new profile with those same permissions.
6. Click **Submit**.
7. On the Web Access Mask, check the box next to the new profile number.
8. To verify or edit permissions, click **Change**.
9. In the column beneath the new profile number, verify that a check is in the box for each Web page (menu item) this profile can access.
10. To name the profile, enter a name in the box next to the profile number at the top of the page.
11. Click **Submit**.

Changing Web profiles

Procedure

1. On Communication Manager Server Administration Interface, navigate to **Security** > **Web Access Mask**.
2. On the Web Access Mask page, check the box next to the profile number to edit.
3. Click **Change**.
4. To provide access to a menu item, on the Change Access Masks page, select the Menu-Item check box.
5. Click **Submit**.

Duplicating Web profiles

About this task

Duplicate an existing profile to create a new profile with similar permissions. See Adding web access profiles on page 88.

Deleting Web profiles

Procedure

1. On the Communication Manager Server Administration Interface, navigate to **Security** > **Web Access Mask**.
2. On the Web Access Mask page, check the box next to the profile number to edit.
3. Click **Delete**.
4. On the Delete Access Mask page, click **Submit**.

Changing the profile base through the Web

About this task

Ensure that no existing Linux groups use the same range as the new set of profiles you are creating.

Procedure

1. On Communication Manager Server Administration Interface, click **Security** > **Web Access Mask**.
2. On the Web Access Mask page, click **Change Access Mask Base** button.
3. Enter the new Access Mask Base number in the box provided.
4. Click **Submit**.

Displaying the profile base on Server Administration Interface

Procedure

1. On Communication Manager Server Administration Interface, click **Security** > **Web Access Mask**.
2. The Web Access Mask page displays the Access Mask base number.

User profiles for Communication Manager SAT access administration

Adding SAT profiles

About this task

Add a Communication Manager SAT profile to define the accessible SAT forms for a user assigned this profile.

Procedure

1. Log in to SAT to access the User-Profile SAT screen.
2. Enter `add user-profile [n|next]`.

3. On the User Profile screen, fill in the following fields:
   - **User Profile Name**

     Optional field, may be used to identify the profile's purpose or use
   - **This profile is disabled**

     Activates, disables the profile. A user assigned to a profile that is disabled is denied all access.
   - **Facility Test Call Notification**

     Enter `y` to have the user receive notification at logoff if Facility Test if Notification is still administered.
   - **Grant un-owned permissions**

     If this profile has write access to the user-profile form, a user with this profile can grant any permission allowed for profile 18 (customer super user) to other profiles even though this profile does not itself have those permissions.
   - **Shell Access**

     Enter `y` to execute **`go shell`** from SAT
   - **Acknowledgment required**

     Enter `y` if you want to logoff while Facility Test Notification is still administered
   - **Extended Profile**

     Enables the extended profile for this SAT profile.
4. Enter `y` in the **Enbl** column opposite the objects (SAT screens) in the **Name** column to allow users with this profile access to the objects.
5. Optionally, use pages 2-x to further define permissions for each SAT screen. See the description of the **`add user-profile`** command in *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, for more information.

   Note:

   The SAT profile form lists all the possible SAT screens in the software regardless of whether the associated feature is enabled, disabled, licensed or not licensed. The profile form will not enable, disable or otherwise modify what is available on the system.

Adding extended profiles

About this task

Extended profiles provide additional access control for vector and station forms.

Procedure

1. At the SAT, enter `add user-profile` or `change user-profile`.

2. Set the **Extended Profile** field to `y`.

   See the description of the **`extended user-profile`** command in *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, for more on the extended profile form.

   If the **Extended Profile** field on the user-profile form is `y` an extended profile may exist even if the vector or station form access is set to “- -” on the standard profile

Duplicating SAT profiles

Procedure

1. At the SAT, enter `duplicate user-profile x`, where *x* is an existing profile.
2. On the User Profile screen, enter the new profile number in the **User Profile** field and submit the form.

Deleting SAT user profiles

Procedure

1. At the SAT, type `remove user-profile n`, where *n* is the number of the profile to delete.

   The system displays User Profile screen.
2. Submit the form.

Deleting extended profile

Procedure

1. At the SAT, type `change user-profile n`, where *n* is the number of the extended profile to delete.
2. Set the **Extended Profile** field to `n` and submit the form.

Displaying the profile base at SAT

Procedure

Enter `display profile-base`.

The system displays the User Profile Base screen and shows the profile base number on the screen.

Exporting SAT profiles

Procedure

At the SAT, with export permissions, enter `export user-profiles`.

All user-defined profiles (20-69) are saved to a tab delimited file in `/var/home/ftp/pub/cmprofiles.txt` . You can edit SAT profile information in Microsoft Excel and import the information back into Communication Manager.

Importing SAT profiles

Procedure

At the SAT, enter `import user-profiles`.

The file in `/var/home/ftp/pub/cmprofiles.txt` is imported. You can import this file to Microsoft Excel and edit. If you want to re-import the changed file into Communication Manager, export the file from Excel to a tab delimited file in `/var/home/ftp/pub/comprofiles.txt`.

Chapter 4: Abbreviated Dialing

Use the Abbreviated Dialing (AD) feature to reduce the number of digits that you must dial to place a call. Instead of dialing the entire number, you dial a short code to access the number. The system then dials the stored number automatically. You can also assign abbreviated dialing buttons to telephones, so that you press a single button to dial frequently called numbers.

Abbreviated Dialing is sometimes called speed dialing.

You can store telephone numbers in four different types of abbreviated dialing lists:

- Personal
- Group
- System
- Enhanced

You can also assign privileged numbers to abbreviated dialing lists. Users can use privileged numbers to place calls to numbers that might otherwise be restricted.

Privileged group-number, system-number, and enhanced-number lists provide access to numbers that usually might be restricted.

The switch type and the version determine which lists are available and how many entries you can have on each list. You can assign up to three AD lists to each user or extension. You can assign any combination of a system list, an enhanced list, and as many as three personal lists or three group lists. The list can also have three group lists. Each entry on an abbreviated dialing list can have as many as 24 characters.

Abbreviated Dialing labeling

Users can administer labels for the AD buttons that appear as softkeys on the following telephones:

- 2420 DCP
- 4600 series
- 6400 series
- 8400 series

These personalized labels appear on the menu display of these telephones.

Abbreviated Dialing on-hook programming

With on-hook programming, you can access the programming mode of the telephone without going off-hook. On-hook programming works with the following telephones:

- 2420 DCP
- 4600 series
- 6400 series
- 8400 series, with enabled speakers

With on-hook programming, signaling changes from dual-tone multifrequency (DTMF) to S-channel. The timeout period for this change is 60 seconds. For non-display telephones, signaling remains DTMF, and the timeout period is 10 seconds.

Detailed description of Abbreviated Dialing

Abbreviated Dialing supports the following types of lists:

- Personal lists

  Use personal lists for users who need their own set of stored numbers. You determine which users have access to a personal list and the size of each list. Either you or the user can assign telephone numbers to personal lists. A personal list is created automatically when you assign the list to an individual telephone. Each user can have as many as three personal lists. You can assign a personal list to an attendant with a data module.
- Group lists

  You can define group lists for groups or departments where members of the group must frequently dial the same numbers. You determine which users have access to group lists. Each user can have access to three group lists. You can program the list, or you can designate a user in each group to program the list. Specify this designated user on the Abbreviated Dialing Group List screen.
- System lists

  You can define one system list for the entire organization. Most administrators assign this list to each telephone, and allow everyone in the organization to use the list. If you allow everyone to use the system list, include only numbers that anyone in your organization has permission to call. For example, you might want to add an emergency telephone number or telephone numbers for other office locations to this list.

  The system list can contain up to 100 entries, and can be changed by a system administrator. An administrator can also customize the button labels displayed on Avaya 2420 and Avaya 4620 telephone sets for these system-list entries.
- Enhanced lists

  You can use enhanced lists for telephone users, data-terminal users, and attendants who need more list entries than the number of entries allowed in group-number and system-

number lists. Two enhanced-number lists are allowed per system, in addition to the system-number list. The enhanced list can contain any number or dial-access code.You administer the enhanced lists and determine which users can access the lists.

Abbreviated Dialing administration

The following tasks are part of the administration process for the Abbreviated Dialing feature:

- Adding Abbreviated Dialing lists
- Assigning telephones for group lists

Related links

Adding Abbreviated Dialing lists on page 97
Assigning telephones for group lists on page 97

Preparing to administer Abbreviated Dialing

About this task

You must complete the following actions before you can administer the Abbreviated Dialing feature:

Procedure

View the Optional Features screen, and ensure that the **Abbreviated Dialing Enhanced List** field is set to `y`.

If the **Abbreviated Dialing Enhanced List** field is set to `n`, your system does not display Enhanced Lists for the Abbreviated Dialing feature. However, you can access the other types of lists.

To view the Optional Features screen, type `display system-parameters customer-options`. Press **Enter**.

For a complete description of the Optional Features screens, see *Avaya Aura® Communication Manager Screen Reference*.

Screens for administering Abbreviated Dialing

Screen name	Purpose	Fields
Abbreviated Dialing List	Add Abbreviated Dialing lists.	• **Size** • **Program Ext**
Station	Define extensions for lists and program buttons used by the Abbreviated Dialing feature.	**Group**

Adding Abbreviated Dialing lists

Procedure

1. Enter `add abbreviated-dialing group next`.
2. In the **Group Name** field, type a name for this list.
3. In the **Size** field, type a number in multiples of 5.

   This number defines the number of entries on the dialing list.

   For example, if you want to store eight telephone numbers in the list, type `10` in the **Size** field.
4. In the **Program Ext** field, type the extension.
5. Type the telephone numbers that you want to store.

   Type one number for each dial code.

   Each telephone number can be up to 24 digits long.
6. Press **Enter** to save your changes.

   You can display the new abbreviated dialing list to ensure that the information is correct. You can also print a copy of the list.

Assigning telephones for group lists

Procedure

1. Type `change station` *n*, where *n* is the extension that you want to assign to the group list.

   Press `Enter`.

   The system displays the Station screen.
2. Click `Next` until you see the **Abbreviated Dialing** area.
3. Type `group` in any of the three **List** fields.

   Press `Enter`.

   The system displays a blank list number field.
4. Type the list number in the list number field.

   When you assign a group list or a personal list, you must also specify the personal list number or the group list number.
5. Press `Enter` to save your changes.

End-user procedures for Abbreviated Dialing

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Programming the Abbreviated Dialing feature

About this task

These instructions apply to most Avaya telephones with display screens, and work with Avaya Aura® Communication Manager release 6.3 or later.

Procedure

1. On your telephone, press the button labeled `Prog` to enter programming mode.

   If your telephone does not have the **Prog** softkey, press the `Menu` softkey and navigate to the **Prog** option.

   The telephone goes off hook and enters the speaker phone mode.

2. Select the softkey/feature button you want to program until you see the label of the softkey you want to display. You will see the message `Change number? Yes = 1 No = 2.`

3. Pick the option you want.

   You will see a message `Enter number:` on the display. Enter the number you want that button to call.

4. Press the `#` key to save your changes.

5. You will see `Enter label` on the display.

   Use the dial pad to enter the label you want. The label can be up to five characters in length.

6. To exit from the **Prog** mode, disconnect your telephone.

   Pressing the **Exit** button does not exit you from programming mode.

   Note:

   If the number you are entering for an Abbreviated Dialing button is an outside number, you must include 9 or any other applicable trunk code. Numbers programmed on softkeys can be up to 24 digits in length.

Considerations for Abbreviated Dialing

This section provides information about how the Abbreviated Dialing feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Abbreviated Dialing feature under all conditions.

- You cannot remove the telephone or disconnect the attendant if the extension belongs to a group-number list.
- When using an AD button to access a messaging system, the user's login and password should not be assigned to the button. The system ignores button entries after the messaging access number.
- You can use an Abbreviated Dialing list at any time during incoming or outgoing calls.

Interactions for Abbreviated Dialing

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

Last Number Dialed

The Last Number Dialed feature redials the same number a user just dialed. This happens even if the user accessed an abbreviated dialing list for the previous call. However, if the last dialed string includes any special characters, these characters are ignored by last-number-dialed call. Examples of special characters might be indefinite wait, mark, pause, suppress, wait and so on.

If the previously-called number is in an AD privileged list, and if you have restricted permission to dial the number because of the class of restriction, you cannot redial the number using Last Number Dialed. To redial the number, you have to access the AD privileged list again.

Remote Access

You can access the System, Group, and Enhanced Abbreviated Dialing lists administered on the Console Parameters screen through the Remote Access feature.

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*.

Edit Dialing

Edit Dialing feature enables you to pre-dial a number when the telephone is on-hook. During the pre-dialing phase, you can edit the digits of a dialed number. The number is dialed when you go off-hook (lifts handset or presses the **speaker** button) or press the **send soft** key.

Edit dialing feature is available on Communication Manager Release 5.2 or later. The 96xx and 96x1 series with IP telephones with H.323 3.0 or later firmware support this feature. This feature is not supported with IP telephones with SIP firmware.

The **Systems Parameter** field on the Feature-Related System Parameters screen in Communication Manager controls this feature for all Edit Dial capable telephones. When enabled, a telephone goes into the Edit Dial mode in the on-hook state. After enabling a telephone, when you press a dial pad button in 96xx and 96x1 telephones, Communication Manager sends a message to Edit Dial capable telephones. This message instructs the firmware to collect digits to send to Communication Manager.

Feature interactions

If you use the telephone dial pad to configure or use the following features, Communication Manager disables Edit Dial. However, when you finish using the dial pad to configure these

features, Communication Manager re-enables Edit Dial. The features listed in this section use on-hook dialing:

- Aux Work Reason Codes
- Automatic Wakeup
- Check In/Out
- Directory
- Do Not Disturb (DND)
- DND Group
- DID View/Remove
- Hotel/Motel Features
- Message Retrieval
- Message Notification On/Off
- Maid Status
- Manual and Clocked Override
- Posted Messages
- VIP Check In

Chapter 5: 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.

Detailed description of Administer location per station

Endpoints with the same Multiple Locations number share characteristics which are in general assigned over large geographic areas: time zone, digit analysis, compounding, call progress tone generation, loss plan, and analog line board parameters. In general, it is to assign one location number with respect to per area code or per major metropolitan area.

The Administer location per station feature adds a **Location** field on the Station screen that overrides most of the location administration associated with the station. The **Location** field is added for H.323 and SIP station types.

Note:

To use the Administer location per station feature with an H.323 softphone, administer the extension as an IP telephone type.

If the **Location** field on the Station screen is not blank, Communication Manager overrides the **Location** field of the following screens:

- Media Gateway
- IP Network Region
- Stations with Off-PBX Telephone Integration screen, only when its **Location** field is blank.

If the **Location** field on the Station screen is blank, Communication Manager uses the following fields for location information:

- The location of the PROCR.
- The location of the IP Network Region for the IP addresses range of the telephone. The range is administered on the IP Network Map screen. The location is administered in the **Location** field of the IP Network Region screen.

- The location of an Off-premises station (OPS) using OPTIM.
  - When the **Location** field on the Stations with Off-PBX Telephone Integration screen is administered to blank, OPTIM stations use the location of the incoming trunk.
  - If the incoming trunk is non-IP, Communication Manager uses the location of the trunk media module.
  - If the incoming trunk is IP, Communication Manager uses the location of the Far-end Network Region administered on the Signaling Group screen.

Administer location per station supported features and screens

The following features and screens use location. The location number can be entered through several SAT screens.

- AAR and ARS Digit Analysis Table
- AAR and ARS Digit Conversion Table
- Agent LoginID
- Automatic Wakeup
- Call Type Digit Analysis Table
- CDR System Parameters
- Dial Plan Analysis Table
- Dial Plan Parameters
- Display Parameters
- Do not Disturb
- Hunt Group
- Location Parameters
- Locations
- Service Hours Table
- Special Applications
  - SA9065 - Crisis Alert to Stations by Location
  - SA9073 - Use Called Party Location for LWC Time/Date
  - SA9004 - Multi-Location Call Routing for IP-DECT
  - SA8904 - Location Based Call Type Analysis
- Station
- System Parameters Call Coverage/Call Forwarding
- Time of Day Coverage Table
- Toll Analysis

- Uniform Dial Plan Table

Station screen behavior after an upgrade

The following occurs after Communication Manager upgrades:

- If the OPS application type on the Stations with Off-PBX Telephone Integration screen for the extension has a location value, the **Location** field on the Station screen is set to the same Stations with Off-PBX Telephone Integration screen value.
- If the OPS application type is not administered on the Stations with Off-PBX Telephone Integration screen for the extension, the **Location** field on the Station screen is blank.

Location number on Station screen administration

The following step is part of the administration process for the Administer location per station feature:

- Setting up location number on Station screen.

For information on how to administer the above tasks, see *Administering Avaya Aura® Communication Manager*.

Screens for administering location number on Station screen

Screen name	Purpose	Fields
Locations	Define location	Disp Parm Loc Parm Rule Timezone Offset
Optional Features	Ensure that the multiple locations feature is enabled.	Multiple Locations
Station	Administer a location to a station.	Location

Interactions for Administer location per station

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

Multinational Location

The Administer location per station feature is frequently used with the Multinational Locations feature.

Emergency Calling

Use the location number on the Station screen with location-based ARS routing to route emergency calls from remote telephones through a PSTN trunk near the telephone.

X-port IP extensions

All Communication Manager features for calls involving X-port IP extensions will use the **Location** field administered on the Station screen.

XDID, XDIDVIP, virtual

The **Location** field is not added to XDID, XDIDVIP, and virtual station screens. XDID and XDIDVIP station types use the location of their hunt-to extensions. Virtual station types use the location of their map-to extensions. However, the locations of hunt-to stations and map-to stations can be based on the **Location** field administered on those Station screens.

Agent Login ID

The Administer location per station feature applies to features invoked by an EAS agent logged in through the telephone.

Automatic Wakeup

Automatic Wakeup works with multiple locations.

Note:

During the wakeup call, the Automatic Wakeup feature uses speech synthesis to report the system time.

Do Not Disturb

Do Not Disturb works with multiple locations.

Time of day coverage

Time of day coverage uses the station's location's time.

Time of day station lock

The Time of day station lock feature uses the system-wide time instead of the station's location's time.

Terminals

SIP telephones can use different information sources for location information compared to other telephones. For information on configuring SIP telephones, see the *Avaya one-X® Deskphone Edition for 9600 Series SIP IP Telephones Administrator Guide*.

Adjunct Switch Applications Interface

The Administer location per station feature applies to features invoked by Adjunct Switch Applications Interface (ASAI).

Call Detail Recording

Call Detail Recording feature is used with the **location-from**, **location-to**, **country-from**, **country-to**, **timezone-from**, and **timezone-to** options of the Multinational Locations feature.

Property Management System

Property Management System can activate or deactivate Do Not Disturb and Automatic Wakeup for a station.

Chapter 6: 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

Use the Administered Connections (AC) feature to administer virtual private-line connectivity over the AT&T Switched Network. Access is over an ISDN trunk group for which the **Service Type** field on the ISDN Trunk Group screen is set to `SDDN` (Software Defined Data Network). The system uses the **Destination** field on the Administered Connection screen to route calls when AC is active, based on associated authorized time-of-day fields.

You can establish an AC between:

- Two endpoints on the same 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 that has the originating endpoint. For an AC in a private network, if the two endpoints are on two different servers, Automatic Alternate Routing (AAR) through ISDN, DS1, or analog tie trunks and intermediate servers are usually used to route the connection. If required, you can also use Automatic Route Selection (ARS) and Generalized Route Selection (GRS) through the public network. The system routes the call over associated ISDN trunks. When the far-end answers, a connection occurs between the far-end and the near-end extension that is administered in the **Originator** field on the Administered Connection screen.

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.

Administered Connections administration

The following task is part of the administration process for the Administered Connections feature:

- Setting up Administered Connections

Related links

[Setting up Administered Connections](#) on page 112

Screens for administering Administered Connections

Screen Name	Purpose	Fields
Data Modules	To administer fields on the Data Modules screen.	All
DS1 Media Module	To administer fields on the DS1 media module screen.	All
Access Endpoint	To administer fields on the Access Endpoint screen.	All
Trunk Group	To administer fields on the Trunk Group screen.	All
Class of Restriction	To administer fields on the Class of Restriction screen.	All
Class of Service	To administer fields on the Class of Service screen.	All
Dial Plan Parameters	To administer fields on the Dial Plan Parameters screen.	**Local Node Number**

Table continues…

Screen Name	Purpose	Fields
Administered Connection	To administer fields on the Administered Connection screen.	All
Station	To assign one button as `ac-alarm`	**Feature Button Assignments** area
Attendant Console	To assign one button as `ac-alarm`	**Feature Button Assignments** area

Setting up Administered Connections

About this task

Note:

For detailed information about the screens that you use in the following procedure, see *Avaya Aura® Communication Manager Screen Reference*.

Procedure

1. In the **Types** field on the Data Modules screen, choose one of the following data module Types.

   Administer all fields that the screen displays for that data module type.

   - Processor/Trunk Data Module. Use with:
     - MPDMs, 700D, 7400B, 7400D, or 8400B
     - MTDMs, 700B, 700C, 700E, or 7400A
   - Processor Interface Data Module. See *Administering Network Connectivity on Avaya Aura® Communication Manager* for more information.
   - 25 Data Module. See *Administering Network Connectivity on Avaya Aura® Communication Manager* for more information.
   - 7500 Data Module. Use with an ISDN Line 12-BRI-S-NT.
   - World Class Core BRI Data Module. Use with wcbri.
2. On the DS1 Circuit Pack screen, administer all fields.

   Use with server node carriers.
3. On the Access Endpoint screen, administer all fields.
4. In the **Group Type** field on the **Trunk Group** screen, choose one of the following Group Types.

   Administer all fields that the screen displays for that group type.

   - 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 Record screen, administer the **Local Node Number** field with a number that matches the distributed communications system (DCS) server node number and the Call Detail Recording (CDR) node number.

   Valid values are 1 to 63.
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

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

- Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), Generalized Route Selection (GRS)
- Abbreviated Dialing

  Use Abbreviated Dialing entries in the **Destination** field on the Administered Connections screen. Entries must comply with restrictions.
- Busy Verification of stations and trunks

  This feature does not apply to access endpoints because access endpoints are used only for data.
- Call Detail Recording (CDR)

  For an AC that uses a trunk when CDR is active, the origination extension is the originator of the call. CDR is unavailable for access endpoints.
- Class of Restriction (COR)

  Reserve a COR for AC endpoints and SDDN trunks to restrict endpoints that are not involved in AC from connecting to SDDN trunks or endpoints that are involved in AC.
- Class of Service (COS) and Call Forwarding

  Assign a COS that blocks Call Forwarding activation at the AC endpoint.
- Data Call Setup

  Do not assign a default dialing destination to a data module when the data module is used in an AC.
- Data Hotline

  Do not assign a hotline destination to a data module when the data module is used in an AC.

- Digital Multiplexed Interface (DMI)

  Use DMI endpoints as the destination in an AC. DMI endpoints do not have associated extensions, so do not use DMI endpoints 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.

- Hunting

  Do not use a hunt group extension as the originating endpoint of an AC.

- Modem Pooling

  If you require a modem in an AC, a modem 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 might 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 use the **`set time`** command to change the system time, 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, the server attempts to establish the AC.

  If any AC, scheduled or continuous, is in retry mode and the system time changes, the server attempts to establish the AC.

- System Measurements

  Access endpoints are not measured. All other trunks in an AC are measured as usual.

- Terminal Dialing

  Turn off terminal dialing for data modules that are used in an AC to prevent display of call-processing messages, such as INCOMING CALL, on the terminal.

- Trunk Groups

  To invoke autorestoration, route an AC over SDDN trunks. Because a successful restoration depends on an SDDN path, keep some SDDN trunks idle.

Chapter 7: Administrable Alternate Gatekeeper List for IP telephones

The Alternate Gatekeeper List (AGL) feature is available on Communication Manager 5.1 and later. Using the Alternate Gatekeeper List (AGL) feature, you can specify the number of IP interfaces for telephones connected within a specific network region.

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

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

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

From Communication Manager 5.1 onwards, H.323 IP telephones in a network region can have an AGL list with no more than 16 members. You can continue to use the AGL feature of prior releases (up to 65 C-LAN/PE members in the AGL), or use the more efficient method of controlling telephone recovery by condensing the number of gatekeepers sent by Communication Manager based on new network region administration.

- If the **AGL** field is set to a numeric value, Communication Manager uses that number of gatekeeper addresses.
- If the **AGL** field is set to all, Communication Manager includes all possible gatekeeper addresses in the endpoint's own network region and in any regions to which the endpoint's region is directly connected.

To use the Communication Manager AGL feature, administrators enter a numeric value in the new **AGL** field of the Inter Network Region Connection Management screen. The Inter Network Region Connection Management screen is used 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 IP (H.323) telephone that is in that source network region. Once the numeric values are entered, Communication Manager

calculates the total number of gatekeepers that are assigned for each destination region. The total AGL assignments for each region must sum to 16 or lower. If an administrator enters a value that makes the AGL assignment greater than 16, the system displays an error message.

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

Note:

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

For more information on the administration procedures for this feature, see *Administering Avaya Aura® Communication Manager*.

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.

AGL high-level capacities

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 7 by adding 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 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 interacts with other features on the system.

- You can have some regions that use the pre-Communication Manager 5.1 non administrable 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.
- 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 PROCRs from the same region and from directly connected regions. The AGL feature included PROCRs from all indirectly connected regions if there were no PROCRS in the same or directly connected regions. With this enhancement, it is now possible to explicitly administer Communication Manager to include PROCRs 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 PROCRs to be eligible to be used for load balancing.
- In general, when using the Communication Manager Administrable AGL feature, PROCR priorities should not be used. Note the following information:
  - For TTS telephones, Communication Manager enhanced feature considers priorities, PROCR socket load, PROCR’s service state, and whether the H.323 IP telephone registration can use PROCRs for load balancing.
  - For non-TTS telephones, priorities and PROCR socket load are taken into account when load balancing.
  - For TTS and non-TTS telephones, the Communication Manager enhanced feature does not take either priorities or PROCR socket load into consideration when building the AGL.

Chapter 8: Administrable Language Displays

Use the Administrable Language Displays feature to display telephone messages in the language of the user. Messages are available in English (the default), French, Italian, Spanish, or one user-defined language that the administrator sets up. To view messages, this feature requires user telephones with a 40-character display.

Communication Manager Release 4.0 or later also supports ISO 8859-1 encoding capability. For more information, see *Administering Avaya Aura® Communication Manager*.

Detailed description of Administrable Language Displays

With the Administrable Language Displays feature, you can select one language for the static messages that telephones and attendant consoles display. The system includes approximately 900 static display messages, such as “Transfer complete.” You can select from English, French, Italian, Spanish, a user-defined language, or Unicode.

The following types of information are pre-translated for display in English, French, Italian, and Spanish. If you select **user-defined**, you must enter a translation for each message.

- Automatic Wakeup
- Adjunct Switch Applications Interface (ASAI)
- Busy Verification of Terminals and Trunks
- Call Appearance buttons
- Call Detail Recording (CDR)
- Call Progress Feedback Displays
- Class of Restriction (COR)
- Date-Time Mode
- Days of the Week
- Months of the Year
- Do Not Disturb

- Enhanced Abbreviated Dialing
- Integrated Directory
- ISDN
- Leave Word Calling
- Malicious Call Trace
- Emergency Access to Attendant
- Queue Status
- Miscellaneous Call Identifiers
- Party Identifiers
- Property Management Interface
- Security Violation Notification (SVN)
- Stored numbers
- Station hunting
- Time-of-Day Routing
- Transfer messages

Unicode display administration

To use Unicode display languages, you must have the appropriate Avaya Unicode Message files loaded on Communication Manager. These files are named `avaya_unicode.txt` (standard phone messages), `custom_unicode.txt` (posted messages and system labels), `avaya_user-defined.txt` (standard phone messages using Eurofont), and `custom_user-defined.txt` (posted messages and system labels using Eurofont).

To use the Phone Message files `avaya_unicode.txt` and `custom_unicode.txt`, you must have Unicode-capable stations, such as the 4610SW, 4620SW, 4621SW, 4625SW, and Avaya Softphone R5.0. Only Unicode-capable stations have the script (font) support that is required to match the scripts that the Unicode Phone Message file uses. To use the user-defined messages files `avaya_user-defined.txt` and `custom_user-defined.txt` you must use an Avaya digital phone that supports Eurofont or Kanafont.

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
- Ukranian

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.

Administrable Language Displays administration

The following tasks are part of the administration process for the Administrable Language Displays feature:

- Setting The display language
- Entering translations for a user-defined language

Related links

Setting the display language on page 124
Entering translations for a user-defined language on page 125

Preparing to administer Administrable Language Displays

About this task

You must complete the following actions before you can administer the Administrable Language Displays feature:

Procedure

1. Ensure that the **Display Character Set** field on the System Parameters Country-Options screen is set to the character type that you want to display.

   Avaya sets this field. If the **Display Character Set** field is not set to the character type that you want to display, go to the Avaya Support website at http://support.avaya.com to open a service request.

2. Ensure that the type of telephone that your company uses has a 40-character display, and supports the characters that you want to display.

   Each character set requires specific telephones. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to Administrable Language Displays.

3. For Unicode display, ensure that the Communication Manager telephone messages for the Unicode display language are loaded.

   The file `avaya_unicode.txt` contains Communication Manager telephone messages. The file `custom_unicode.txt` contains Communication Manager posted messages and system labels. You can load these files when you upgrade or install the system. You can also download these files at any time from the Avaya support website http://www.avaya.com/support.

   The Avaya Excel Translation Editor for creating Unicode translations requires Microsoft Excel 2000 or above.

4. To support Unicode on the 4620SW IP telephone, you must:

   - Install the appropriate version of firmware on the telephone
   - Set the language

   For more information on administering telephones, see the *4600 Series IP Telephone R2.0 LAN Administrator's Guide* and the *4620/4620SW IP Telephone R2.0 User's Guide*.

Screens for administering Administrable Language Displays

Screen Name	Purpose	Fields
System Parameters - Country Options	Select the appropriate character set for the language that you want to use	**Display Character Set**
Attendant Console	Select the appropriate display language	**Display Language**
Language Translations	Enter user-defined translations of messages	**Translation**

Setting the display language

Procedure

1. Type `change attendant n`, where *n* is the number of the attendant console that you want to change.
2. In the **Display Language** field, type the name of the display language that you want to use.

   Note:

   The Display Language value unicode is available only for station type 4620SW or 4610SW.

3. Select `Enter` to save your changes.

Entering translations for a user-defined language

Procedure

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

   The system displays the Attendant Console screen.
2. In the **Display Language** field, type `user-defined`.
3. Press `Enter` to save your changes.
4. Type `change display-messages n`, where *n* is the message for which you want to translate the display language.

   Click `help` to view the messages that you can choose to translate. Press `Enter`.

   The system displays the Language Translations screen for the type of message that you want to translate.
5. In the `Translation` field, type the translation of the message in the user-defined language.
6. Press `Enter` to save your changes.

   For more information on telephone displays, see *Administering Avaya Aura® Communication Manager*.

Considerations for Administrable Language Displays

This section provides information about how the Administrable Language Displays feature behaves in certain circumstances.

Note:

The considerations stated here apply only to the ISO 8859-1 encoding capability.

- The ASCII (0x00 – 0x7F) does not require any conversion.
- The range 0x80 – 0x9F is not supported when Display Character Set on the System Parameters Country-Options screen has the value **Roman**.
- If CID is sent through a tandem server, the CID could display incorrectly on the server where the call terminates if that server does not support 8859-1/Eurofont conversion, or if the QSIG trunk does not have the conversion feature enabled.
- If Communication Manager receives a name in the simple name form from another vendor and if that name contains accented characters, the name will not display correctly. This is because Communication Manager expects a simple name to use the Eurofont character set.
- It is a known issue that this design does not properly handle names received in the extended name form in character sets other than 8859-1. For such cases, the characters outside the ASCII range will be improperly mapped to Eurofont resulting in an incorrect name display.

The following list describes the situations when the Display Messages screen is disabled:

- After loading an `avaya_user-defined.txt` file, Communication Manager disables the following qualifiers for both the change and display display-message commands:
  - ad-programming, malicious-call-trace, softkey-labels, auto-wakeup-dn-dst, miscellaneous-features, time-of-day-routing, button-labels, transfer-conference, call-identifiers, property-management, view-buttons, date-time, self-administration, vustats, and leave-word-calling.
- After loading an `avaya_user-defined.txt` file, Communication Manager disables the page 1 of the Posted Messages screen for both the change and display display-message commands. However, you can enter translations for the fixed languages in the Posted Messages screen.
- After loading a `custom_user-defined.txt` file, Communication Manager disables the last page of the Posted Messages screen and relates to the user-defined translation for both the change and display display-message commands. You can, however, enter translations for the fixed languages in the Posted Messages screen.
- After loading an `avaya_user-defined.txt` file, Communication Manager disables the user-defined keyword for the **Label Language** field on the Abbreviated Dialing screen. You can, however, enter translations for the fixed languages in the Abbreviated Dialing screen.

Administrable Language Displays troubleshooting

This section lists the known or common problems that users might experience with the Administrable Language Displays feature.

Problem	Possible cause	Action
The system displays the characters that you have not entered.	This feature is case sensitive.	Check the table to ensure that you entered the characters in the correct case.
You have entered a lowercase *c*, but the system displays an asterisk (*).	Lowercase *c* has a specific meaning in Communication Manager. Therefore, you cannot map *c* to any other character. The system displays an asterisk (*) in its place.	Use a different letter for this character mapping.
You have entered ~–> or ~<– but the system displays no value.	These characters do not exist as single keys on the standard US English keyboard. Therefore the system is not programmed to handle these characters.	Check the model of the keyboard that you are using.

Table continues…

Problem	Possible cause	Action
The system displays the enhanced characters in the fields that you did not update.	If an existing display field contains a tilde (~) that is followed by Roman characters, and you update and submit that screen, that field displays the enhanced character set.	Remove the existing tilde before you submit the screen.
The terminal displays nothing at all.	Some unsupported terminals do not display anything if a special character is presented.	Check the model of the display terminal that you are using.
You entered a character with a descender and part of the descender is cut off in the display.	Some of the unused characters in Group2a have descenders that are not visible entirely within the display area. These characters are excluded from the character map.	Use Group1 equivalents for the letters g, j, p, q, and y.

Chapter 9: Administration Change Notification

Use the Administration Change Notification feature to notify adjunct systems when administration data on Communication Manager is changed. These notifications keep a client application that is running on an adjunct, such as Enterprise Directory Gateway, synchronized with Communication Manager.

Communication Manager uses Administration Change Notification to communicate with the Avaya Directory Enabled Management (DEM) client. This feature provides you with real-time, integrated, directory-based, read-write access to Communication Manager administration data. This access is based on rules that you define. With Administration Change Notification, you can subscribe to notifications whenever the administration data changes in Communication Manager. This feature also provides real-time updates whenever the administration data changes in a particular object, such as a telephone.

Detailed description of Administration Change Notification

Use the Administration Change Notification feature to track changes that are made through the System Access Terminal (SAT), INADS port, a Property Management System (PMS), a Call Management System (CMS), Avaya Network Administration, or Avaya Directory Gateway. The Administration Change Notification feature also tracks any changes that are made through a telephone interface, such as Terminal Translation Initialization (TTI), Personal Station Access (PSA), and Terminal Self Administration.

Communication Manager only notifies the adjunct about a change to a data object. To obtain details about the change, the adjunct must request this information from the server over a separate link.

Administration Change Notification administration

The following task is part of the administration process for the Administration Change Notification feature:

- Initiating Administration Change Notification

Related links

Initiating Administration Change Notification on page 129

Screens for administering Administration Change Notification

Screen Name	Purpose	Fields
Administration Changes	View changes to administration data in Communication Manager.	All

Initiating Administration Change Notification

Procedure

From the client application, enter `notify history`.

Communication Manager continues to send change notification over the Operations Support System Interface (OSSI) link until you cancel the command.

Chapter 10: Administration Without Hardware

Use the Administration Without Hardware (AWOH) feature to administer telephones that are not yet physically on the system. Like administration with hardware, the system preserves all features that the user has activated, such as Call Forwarding and Send All Calls, when you move a telephone. This greatly speeds the process of setting up and making changes to telephones on your system.

Detailed description of Administration Without Hardware

With AWOH you can enter telephone translations without assigning ports. Therefore, AWOH streamlines system initialization, major additions, and rearrangements or changes You can add or change a Station screen, and you can store duplicated telephones without specifying a port location.

Use the **`list configuration circuit-pack`** *board code* command to list the circuit packs that require firmware downloads. However, this command does not display circuit packs that are logically administered (Administration Without Hardware - AWOH) or are unplugged.

Physical characteristics of an AWOH telephone

AWOH telephones cannot generate alarms or errors, because the physical telephones or data terminals are not associated with a Station screen. Neither the system nor other telephones or data terminals can affect the lamp or the alerting tones of an AWOH telephone. If TTI is disabled and a user presses the dialpad buttons or uses data terminal that does not have an associated Station screen, the action has no effect on system operation.

User-activated features with AWOH

When someone moves a telephone or a data terminal, the user-activated features, such as Call Forwarding and Send All Calls, remain active. Any action that changes the lamps or the status of the telephone is reflected when the telephone or the data terminal is again associated with a Station screen.

Association and disassociation with AWOH

Telephone users, data-terminal users, and technicians can disassociate telephone translations from the current terminal port, and then associate the telephone translations with another terminal port. Users use the Personal Station Access (PSA) feature to disassociate and associate telephones. Technicians use the Terminal Translation Initialization (TTI) feature to disassociate and associate telephones.

An AWOH telephone is considered to be disassociated when no hardware port is assigned to the telephone. To indicate that no hardware is associated with a telephone, type `x` in the **Port** field of the appropriate screen. When the port is assigned later, the AWOH telephone is considered to be associated.

Phantom extensions

You can use phantom extensions to provide call coverage, including Avaya Aura® Messaging and Avaya Messaging coverage, for users who do not have telephones or data terminals that are physically associated on the server.

You can also use phantom extensions for the automatic call distribution (ACD) Dialed Number Identification Service (DNIS). With ACD DNIS, you can administer a phantom extension on the switch for each type of call that ACD agents need to identify.

To use ACD DNIS, either a user with console permissions forwards the phantom extension to an ACD split, or the coverage path of the phantom extension includes an ACD split. The **Name** field for the phantom extension identifies the service that the caller wants. The agent then uses this information to address the caller properly.

Administering Administration Without Hardware

The following tasks are part of the administration process for the Administration Without Hardware (AWOH) feature:

- Assigning AWOH for a hunt group queue
- Assigning AWOH to a telephone
- Assigning AWOH to an attendant console
- Assigning AWOH to a data module

Related links

Assigning AWOH for a hunt group queue on page 132
Assigning AWOH to a telephone on page 133
Assigning AWOH to an attendant console on page 133
Assigning AWOH to a data module on page 133

Screens for administering Administration Without Hardware

Screen name	Purpose	Fields
Attendant Console	Assign a port to the attendant console.	**Port**
Data Module	Assign a port to the data module.	**Port**
Hunt Group	Assign port information for a queue.	• **Calls Warning Port** • **Time Warning Port**
Station	Assign a port to a telephone.	`Port`

Assigning AWOH for a hunt group queue

Procedure

1. Type `change hunt-group` *n*, where *n* is the number of the hunt group to which you want to assign AWOH. Press `Enter`..

   The system displays the Hunt Group screen.

2. In the **Calls Warning Port** field, type `x`.

   Note that the system displays the **Calls Warning Port** field if the **Queue** field is set to `y`.

3. When you type `x` in the **Calls Warning Port** field, the system displays an **Extension** field.

   In the **Extension** field, type an extension that a technician can use, along with TTI, to assign a port number from the actual port. When a technician or an administrator assigns a port number, the system removes the extension, and the extension becomes unassigned. An administrator uses the **`change hunt-group`** command to assign the port number.

4. In the **Time Warning Port** field, type `x`.

   Note:

   Note that the system displays the **Time Warning Port** field if the **Queue** field is set to `y`.

5. When you type `x` in the In the **Time Warning Port** field, the system displays an **Extension** field.

   In the **Extension** field, type an extension that a technician can use, with TTI, to assign a port number from the actual port. When a technician or an administrator assigns a port number, the system removes the extension, and the extension becomes unassigned. An administrator uses the **`change hunt-group`** command to assign the port number.

6. Press `Enter` to save your changes.

Assigning AWOH to a telephone

Procedure

1. Type `change station n`, where *n* is the number of the extension to which you want to assign AWOH. Press `Enter`.
2. In the **Port** field, type `x`.
3. Press `Enter` to save your changes.

Assigning AWOH to an attendant console

Procedure

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

   The system displays the Attendant Console screen.
2. In the **Port** field, type `x`.
3. Press `Enter` to save your changes.

Assigning AWOH to a data module

Procedure

1. Type `change data-module n`, where *n* is the number of the data module to which you want to assign AWOH. Press `Enter`.

   The system displays the Data Module screen.
2. In the **Port** field, type `x`.
3. Press `Enter` to save your changes.

Interactions for Administration Without Hardware

This section provides information about how the Administration Without Hardware (AWOH) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of AWOH in any feature configuration.

- Association and disassociation interactions
  - Attendant

    An attendant cannot disassociate the attendant telephone if the attendant has a call in a queue, a call on hold, or a call that is active. An attendant cannot dissociate the attendant telephone under those conditions, even if the attendant is in Position Available mode.
  - Attendant Night Service

A night service telephone cannot be removed while the telephone is in night service. See the “Night Service” feature for more information.

- Attendant Release Loop Operation

  The system reclassifies calls as attendant group calls if the attendant holds the calls with the release loop operation, and if the attendant disassociates the attendant telephone before the attendant timed-reminder interval expires.

- Automatic Callback

  If a telephone becomes disassociated while another telephone has automatic callback active for the disassociated telephone, the automatic callback light turns off. The callback sequence does not occur for the telephone that has automatic callback active.

- Bridged Call Appearance

  If a telephone has a bridged call appearance of an off-hook telephone, the first telephone can disassociate at any time, and not disrupt a call that is in progress on the bridge.

  If a telephone with a bridged call appearance associates itself while the extension for the bridged appearance is on a call, the associated telephone can join the call.

  You cannot disassociate a telephone from a bridged call appearance. You must disassociate a telephone from the port on which the telephone resides.

- Call Coverage

  If an AWOH telephone disassociates while Send All Calls or Go to Coverage is active, both features remain active.

- Call Coverage Answer Group

  If a technician or an administrator associates a telephone, the telephone cannot join calls that are in progress at the call-coverage answer group. The telephone can join subsequent calls.

- Call Forward

  A telephone can disassociate while Call Forwarding is active.

  If a Call Forwarding destination disassociates, Call Forwarding to that extension remains active.

- Call Park

  If a line appearance is available, a user can disassociate while a call to that telephone is parked. The user can then retrieve the call from another telephone.

- Call Pickup

  If a line appearance is available, a member of a Call Pickup group can disassociate a telephone at any time.

  If a call is in progress to any extension in a pickup group, any member of the group can disassociate or associate a telephone. The pickup group member who dissociates or associates a telephone does not join the group for the call in progress. The member can participate in subsequent calls.

- Customer-premises equipment (CPE) Alarm

  If a telephone that is administered with a CPE alarm becomes associated with a port while an alarm is active, the telephone receives the alarm when the telephone is associated.

- Hunt Group with Uniform Call Distribution (UCD) and Direct Department Calling (DDC)

  If a technician or an administrator associates a telephone, the telephone cannot join calls that are in progress at the hunt group. The telephone can join subsequent calls.

- Hold

  A telephone user can place a call on hold. The user can then disassociate the telephone, associate the telephone, and retrieve the call that the user placed on hold.

- Intercom Group - Auto/Dial

  See the “Data Call Setup” feature for more information.

- Message Light

  You do not need to delete messages before you dissociate a telephone. If a telephone receives messages while the telephone is disassociated, the system updates the message light when someone associates the telephone.

- Send All Calls

  Send All Calls remains active when a telephone is disassociated.

- Station-to-Station Call

  You cannot disassociate a telephone while someone is active on a call at the telephone.

- Terminating Extension Group (TEG)

  If a technician or an administrator associates a telephone, the telephone cannot join calls that are in progress at the TEG. The telephone can join subsequent calls.

- Transfer

  After user A successfully uses the Transfer feature to connect a caller with user B, user A can dissociate the telephone, the system processes the call between the caller and the transferred-to user as a station-to-station call.

- Trunk Group Night Service

  You disassociate a night service destination that is a telephone the same way that you disassociate a telephone that is not a night service destination. See the “Data Call Setup” feature for more information.

  You disassociate a night service destination that is an attendant the same way that you disassociate an attendant that is not a night service destination. See the “Attendant” feature for more information.

• Attendant interactions

  - Attendant Group

If all attendants of a group use AWOH consoles, internal callers receive ringback tone indefinitely. Attendant AWOH consoles operate the same way as AWOH telephones in group interactions.

- Attendant Override

  When an attendant activates Attendant Override, the attendant hears a busy signal for calls to AWOH extensions, and the attendant bypasses Call Coverage for the extensions.

- Attendant Return Call

  If the attendant extends a call to a telephone, and then the attendant dissociates the attendant telephone before the system returns the call to the attendant, the system reclassifies the call. The system reclassifies the call as an attendant group call, and routes the call to an attendant group.

- Emergency Access to Attendant

  A caller receives a busy signal if:

  - The Emergency Access feature to the attendant is active.
  - All attendants use AWOH consoles.
  - No backup extension is administered.
  - The backup extension is also an AWOH extension.

- Interposition Calling, Attendant to Attendant

  A caller receives the intercept tone for a call to an attendant who has an AWOH console.

- Night Station Service

  A caller receives a busy signal if the attendant activates Night Station Service, and the night service endpoint in an AWOH extension.

- Serial Calling

  With a serial call, the attendant is not in a busy state after the attendant releases a call. Because the attendant is not in a busy state, the attendant can disassociate the attendant telephone.

  If the attendant extends a call to a telephone, and then the attendant dissociates before the system returns the call to the attendant, the system reclassifies the call. The system reclassifies the call as an attendant group call, and routes the call to an attendant group.

  When an attendant attempts to extend a call to an AWOH extension, the attendant hears a busy signal.

- Data Modules

  Users can use the following methods to associate and disassociate data modules:

  - Data-terminal dialing
  - Telephone dialing
  - Other devices

The devices include the use of a default set type to associate, and then remove the default set type, and replace the default set type with the proper data endpoint.

Because digital-terminal data modules (DTDMs) reside on some telephone types, the port is automatically inherited from the host telephone. The DTDM receives a port identification when the telephone associates or disassociates.

- Administered Connections

  If you administer a connection without hardware translation, the system attempts to establish a connection only when both endpoints are associated with hardware translation.

  You disassociate an administered connection when you type x in the **Port** field on the Data Module screen. A technician uses Terminal Translation Initialization (TTI) to disassociate an administered connection.

- Hunt Group - Uniform Call Distribution (UCD) and Direct Departmental Calling (DDC)

  See the “Call Coverage” feature for more information.

- Terminal-to-Data Module Call

  See the “Data Call Setup” feature for more information.

- Transfer

  See the “Transfer” feature for more information.

• Data-terminal interactions

- Administered Connections

  An administered connection endpoint can be an AWOH extension.

- Data Call Setup

  • Data Terminal Dialing

    A keyboard-dialed call that terminates to a data endpoint that is an AWOH telephone, causes a BUSY message on the screen. A busy signal indicates that the terminal is in use, out of service, or AWOH.

  • Telephone Dialing

    See the “Data Call Setup” feature for more information.

- Hunt-Group (UCD and DDC)

  See the “Call Coverage” feature for more information.

- Incoming Destination

  If the incoming destination is an AWOH extension, the caller hears ringback tone from the central office (CO). The system routes incoming calls based on features that are active for the extension. These features include, for example, Call Forwarding and Call Coverage.

- Terminal-to-Data Module Call

If a data endpoint is an AWOH telephone, the caller either sees a BUSY message on the screen or hears a busy signal, depending on the originating hardware. See the “Data Call Setup” feature for more information.

- Telephone interactions
  - Abbreviated Dialing

    AWOH does not change any aspect of the Abbreviated Dialing feature.

    A telephone that has Abbreviated Dialing active, and then becomes disassociated, retains the abbreviated dialing list entries.
  - Automatic Call Distribution

    A user cannot log an AWOH telephone into an Automatic Call Distribution (ACD) split. The user can log on directly or use a Bridged Call Appearance.
  - Automatic Callback

    A user cannot activate the Automatic Callback feature for a call to an AWOH extension. If a user attempts to use the Automatic Callback feature for a call to an AWOH extension, the system sends the reorder tone to the user.
  - Bridged Call Appearance

    A user can use a bridged call appearance of an AWOH extension to place a call.

    A user can use a bridged call appearance of an AWOH extension to answer a call to the AWOH telephone.

    An AWOH extension can contain a bridged call appearance, but a user cannot use the bridged call appearance on the AWOH telephone to place a call.
  - Busy Verification of Terminals and Trunks

    When you use busy verification of terminals and trunks on an AWOH extension, you see the telephone as an out-of-service telephone.
  - Call Coverage

    AWOH telephones interact with Call Coverage as if all call appearances are busy.

    Call Coverage can be active at a disassociated telephone.
  - Call Forward

    Call Forwarding can be active at an AWOH telephone, while the telephone is in a disassociated state. When the extension is associated, Call Forwarding is active.
  - Call Park

    A call to an AWOH extension can be parked only if the primary extension has a bridged call appearance on a non-AWOH telephone. A call that is parked from a bridged call appearance is parked on the primary extension.
  - Call Waiting Termination

    Call Waiting Termination can be administered on a single-line AWOH extension, but the caller receives a busy signal if the extension is disassociated.

- Customer-Provided Equipment (CPE) Alarm

  If a CPE alarm is active for an AWOH extension, no equipment is available to ring or light.

- Data Buttons

  Data buttons are not lit for AWOH data modules.

- Display

  The AWOH feature does not change the display for calls that originate or terminate from a bridged call appearance for an AWOH extension.

- Facility Busy Indication

  A telephone can have a busy indicator light for an AWOH extension, but the light is not lit. The light is not lit because Facility Busy Indication indicates whether an extension is off-hook or on-hook, even if you assign bridged appearances. An AWOH extension is always on-hook.

  You can administer a busy indicator light on AWOH extensions. When an administrator or a technician assigns a port to the extension, the busy indicator light functions as usual.

- Incoming Destination

  If the incoming destination is an AWOH extension, the caller hears ringback tone from the central office (CO). The system routes incoming calls based on features that are active for the extension, such as Call Forward and Call Coverage.

- ISDN-BRI voice terminals

  If TTI is enabled, you cannot use the SAT to enter `x` in the **Port** field of a BRI telephone Station record that is already connected to the switch. Instead, you must dial the TTI disassociate code from the telephone. For more information, see the “Terminal Translations Initialization (TTI)” feature.

- Leave Word Calling

  You can leave a leave-word-calling message at an AWOH extension.

- Manual Message Waiting

  When a user activates Manual Message Waiting toward an AWOH extension, no telephone exists on which to light the message waiting lamp. However, once the AWOH extension is associated with a port or telephone, the message waiting lamp lights.

- Manual Signaling

  Manual Signaling to an AWOH extension has no effect on system operation, because no terminal exists to signal.

  The system does not send a message to the originator of the call to inform the caller that the extension is an AWOH extension, and therefore cannot receive the signal.

- Personal Central Office Line (PCOL)

  You can administer AWOH extensions with PCOL. If a call terminates at an AWOH extension that does not have Call Coverage active, the caller receives ringback tone.

The ringback tone indicates that the call is unanswered. If the AWOH extension has Call Coverage active, the system routes the call to coverage.

- Priority Calling

  A user who sends a priority call to an AWOH extension hears a busy signal.

- Send All Calls

  Send All Calls remains active on AWOH extensions.

- Station Hunting

  You can assign an AWOH extension to a telephone hunting chain.

- Station-to-Station Call

  The system processes a call to an AWOH extension in the same way that the system processes a call to a telephone for which all call appearances are busy.

- Transfer

  The system processes a transfer to an AWOH telephone in the same way that the system processes a call to a telephone that is busy.

Chapter 11: Avaya Aura® Media Server

Avaya Aura® Media Server is used by Communication Manager to provide IP audio capabilities similar to legacy H.248 media gateways or port networks with media processors.

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:

- 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.

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® MS using 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
```

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
```

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.

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
```

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
```

Chapter 12: 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.

Detailed description of Alerting Tone for Outgoing Trunk Calls

This feature provides the capability to apply an alerting tone to an outgoing trunk call after an administrable amount of time. The amount of time that elapses before the alerting tone is applied to the call can be specified, and varies from 2 to 999 minutes. If the timer field is blank (the default value), the feature is disabled and the alerting tone is not applied to the call.

To set the outgoing trunk alerting timer, the system uses the Class of Restriction (COR) of the outgoing trunk group or the originating station. The value in the **Use Trunk COR for Outgoing Trunk Disconnect/Alert** field determines which of these CORs is used. However, the timer does not apply to incoming trunk calls that connect to outgoing public network trunks, with the exception of remote access.

The outgoing trunk alerting timer starts after the called party connects to the trunk. The outgoing trunk call is considered answered if:

- The network provides an answer supervision line signal.
- An ISDN CONNect message is received.
- The Answer Supervision Timeout timer expires.
- The call classifier classifies the call as answered.
- The Outgoing End of Dial Timer expires.

The alerting tone is applied to the call upon expiration of the outgoing trunk alerting timer. The tone is heard by all parties on the call and is repeated at a specified interval until the call ends. The interval is determined by the administration of the **Trunk Alerting Tone Interval (seconds)** field.

The outgoing trunk alerting timer is cancelled if the outgoing trunk drops or is dropped before the timer expires.

The outgoing trunk alerting timer only affects outgoing public network trunks (CO, DIOD, FX, WATS, and ISDN public-network).

Important:

You must not enable outgoing trunk disconnect and outgoing trunk alerting timers at the same time. If you try to administer both timers, the system displays the following message:

```
Cannot enable both Outgoing Trunk Disc and Outgoing Trunk Alert
timers
```

Alerting Tone for Outgoing Trunk Calls administration

The following tasks are part of the administration process for the Alerting Tone for Outgoing Trunk Calls feature:

- Setting the outgoing trunk alerting timer
- Setting the trunk alerting tone interval

For information on how to administer the above tasks, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Alerting Tone for Outgoing Trunk Calls

Screen name	Purpose	Fields
Class of Restriction	Specify when the initial alerting tone must be applied to the call.	Outgoing Trunk Alerting Timer (minutes)
Feature-Related System Parameters	Specify interval at which the alerting tone is repeated on the call.	Trunk Alerting Tone Interval (seconds)

Interactions for Alerting Tone for Outgoing Trunk Calls

This section provides information about how the Alerting Tone for Outgoing Trunk Calls feature interacts with other features in your system. Use this information to ensure that you receive the maximum benefits of the Alerting Tone for Outgoing Trunk Calls feature.

Authorization Codes

For outgoing trunk calls requiring Authorization Codes, the outgoing trunk alerting timer is set based on the COR of the Authorization Code.

Automatic Route Selection

The outgoing trunk alerting timer does not apply to outgoing trunk calls that are emergency or service calls. Specifically, the outgoing trunk alerting timer does not apply to the following ARS call types: alrt, emer, nsvc, op, svcl, svfl, svct or svft.

Bridged Appearances

If a station is on a bridged appearance when making an outgoing trunk call, the outgoing trunk alerting timer is set based on the COR assigned to the primary extension of the bridged appearance, unless you administer the system to use the trunk COR.

Conference

When an outgoing trunk is added to a conference call, the outgoing trunk alerting timer is set based on the COR of the controlling party, unless you administer the system to use the trunk COR. The outgoing trunk alerting timer remains active for the trunk even if the controlling party drops out of the call.

Disability Access

To accommodate individuals with accessibility issues, set the outgoing trunk alerting timer to a large value to provide users with adequate response time.

Emergency Calling

The outgoing trunk alerting timer does not apply to emergency calls.

Expert Agent Selection

If an outgoing trunk call is made from an agent, the outgoing trunk alerting timer is set based on the COR of the agent, not the COR of the station, unless you administer the system to use the trunk COR.

Off-net Call Coverage or Call Forwarding

If a station-to-station call is redirected to a destination on the public network through Off-net Call Coverage or Call Forwarding, the outgoing trunk call is subject to the outgoing trunk alerting timer. The outgoing trunk alerting timer is set based on the COR of the calling party, unless you administer the system to use the trunk COR.

Personal Station Access

If the COR for Personal Station Access (PSA) Dissociated Sets is assigned and an outgoing trunk call is made from a dissociated phone, the outgoing trunk alerting timer is set based on the PSA COR.

Remote Access

If a call originating from a remote access extension accesses an outgoing public network trunk, the outgoing trunk alerting timer is set based on the barrier code COR or authorization code COR, depending upon administration of the Remote Access.

Station Lock

If a locked station makes an outgoing trunk call, the outgoing trunk alerting timer is set based on the Station Lock COR.

System Time

If the System Time changes while the timer is running, the outgoing trunk alerting timer is not cancelled or changed.

Tone for Internal Users Only

The outgoing trunk alerting timer (minutes) is not applicable when **Internal Users Only** field is enabled.

For more information, see Alerting Tone for Internal Users Only on page 151

Tones

If a tone is being applied to a call, the tone must be disconnected to apply the alerting tone. The tone is reapplied to the call after the alerting tone is played.

Transfer

When a call is transferred to an outgoing trunk, the outgoing trunk alerting timer is set based on the COR of the party initiating the transfer, unless you administer the system to use the trunk COR.

If a station transfers an outgoing trunk call to another station, the outgoing trunk alerting timer will not be reset after the transfer. The timer from the start of the original call remains active for the trunk.

Trunk Access Codes

The outgoing trunk alerting timer applies to outgoing trunks accessed through a trunk access code.

Chapter 13: Alerting Tone for Internal Users Only

Use the Trunk Alerting Timer feature to play an zip tone for outgoing and incoming trunk calls for Internal Users Only after an administrable amount of time.

Detailed description of Alerting Tone for Outgoing and Incoming Trunk Calls

This feature enables users to apply zip tone to outgoing and incoming trunk calls after an administrable amount of time. It is applicable for **Internal Users Only**. Users can specify the amount of time before the zip tone applied, ranging from 0 to 999 minutes. If the **Internal Users Only** field is set to `N`, the zip tone for Internal Users Only will be disabled.

To set the outgoing and incoming trunk alerting timer, Avaya Aura® Communication Manager uses the Class of Restriction (COR) of the outgoing or incoming trunk group.

The outgoing and incoming trunk alerting timer starts after the called party connects to the trunk. The trunk call is considered as answered if:

- The network provides an answer supervision line signal.
- An ISDN CONNect message is received.
- The Answer Supervision Timeout timer expires.
- The call classifier classifies the call as answered.

The zip tone is applied to the call upon expiration of the trunk alerting timer. The tone is heard by internal users only and is repeated at a specified interval until the call ends. The interval is determined by the administration of the **Trunk Alerting Tone Interval (seconds)** field.

The trunk alerting timer is cancelled if the outgoing or incoming trunk drops or is dropped before the timer expires.

The trunk alerting timer only affects outgoing or incoming public network trunks such as trunks with the **Service Type** field as public-ntwrk. This is regardless of the trunk group type as SIP, ISDN, WATS, Tandem, or Tie.

Alerting Tone administration for Internal Users Only

The following tasks are part of the administration process for the zip tone for outgoing and incoming trunk calls feature:

- Setting the trunk alerting timer
- Setting the trunk zip tone interval

For information on how to administer the above tasks, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Alerting Tone for Internal Users Only

Screen name	Purpose	Fields
Class of Restriction	Specify when the initial zip tone must be applied to the call.	Trunk Alerting Timer (minutes)
Feature-Related System Parameters	Specify interval at which the zip tone is repeated on the call.	Trunk Alerting Tone Interval (seconds)

Interactions for Alerting Tone for Internal Users Only

This section provides information about how the zip tone for Trunk Calls feature for internal users interact with other features in your system. Use this information to ensure that you receive the maximum benefits of the zip tone for Trunk Calls feature for internal users only.

Authorization Codes

For trunk calls requiring Authorization Codes, the trunk alerting timer is set based on the COR of the Authorization Code.

Automatic Route Selection

The trunk alerting timer does not apply to outgoing trunk calls that are emergency or service calls. Specifically, the trunk alerting timer does not apply to the following ARS call types: alrt, emer, nsvc, op, svcl, svfl, svct or svft.

Bridged Appearances

If a station is on a bridged appearance during a trunk call, the system sets the trunk alerting timer based on the COR assigned to the primary extension of the bridged appearance, unless you configure the system to use the trunk COR.

Conference

When a public trunk call is added to a conference call, the trunk alerting timer is set based on the Class of Restriction (COR) of the first public-trunk party added to the call. On the other hand, the tone repetition timer is based on the **Trunk Alerting Tone Interval (seconds)** field in the

system parameter features form, and it will continue to play at the interval administered in the system parameter features screen, regardless of any additional public-trunk calls added to the conference. The trunk alerting timer remains active until all the parties connected via public-trunk drop from the conference call.

Disability Access

To accommodate individuals with accessibility issues, set the trunk alerting timer to a large value to provide users with adequate response time.

Emergency Calling

The trunk alerting timer does not apply to emergency calls.

Expert Agent Selection

If an agent receives a call from a public trunk or an agent makes a call to a public trunk, playing a zip tone to an agent depends on the Class of Restriction (COR) of the public trunk and not on the agent.

Off-net Call Coverage or Call Forwarding

If a station-to-station call is redirected to a destination on the public network through Off-net Call Coverage or Call Forwarding, the trunk call is subject to the trunk alerting timer. The trunk alerting timer is set based on the COR of the calling party, unless you administer the system to use the trunk COR.

Outgoing Trunk Alerting Timer

This feature is disabled when the **Internal Users Only** field is enabled.

Outgoing Trunk Disconnect Timer

This feature is disabled when the **Internal Users Only** field is enabled.

Personal Station Access

If the COR for Personal Station Access (PSA) Dissociated Sets is assigned and a trunk call is made from a dissociated phone, the trunk alerting timer is set based on the PSA COR.

Remote Access

If a call originating from a remote access extension accesses a public network trunk, the outgoing trunk alerting timer is set based on the barrier code COR or authorization code COR, depending upon administration of the Remote Access.

Service Observe

When the **Internal Users Only** field is activated, and an internal user either receives a call from a public trunk or makes a call to a public trunk, the user will hear a zip tone at regular intervals, which is determined by the **Trunk Alerting Tone Interval**.

However, when a **Service Observer** starts monitoring an internal user's call, both Service Observer tones and the Trunk Alerting Tone will be played intermittently based on a first come, first served basis. If, by any chance, the timers for both types of tones expire nearly simultaneously, the tone that was activated later will be given priority, and it will be played to the user.

Station Lock

If a locked station makes an outgoing trunk call, the outgoing trunk alerting timer is set based on the Station Lock COR.

System Time

If the System Time changes while the timer is running, the trunk alerting timer is not cancelled or changed.

Tones

When an internal user engages in a call with a public trunk user and hears the trunk alerting tone, and if the system needs to play additional brief tones like bridging or conference tones, it will be played based on a first-come, first-served basis. For instances, if the timer for the trunk alerting tone expires, and the Communication Manager needs to play a conference tone at that moment, it will overwrite the internal tone, and vice versa.

Transfer

When a call is transferred to a trunk, the trunk alerting timer is set based on the COR of the party initiating the transfer, unless you administer the system to use the trunk COR.

If a station transfers a trunk call to another station, the trunk alerting timer will not be reset after the transfer. The timer from the start of the original call remains active for the trunk.

Trunk Access Codes

The trunk alerting timer applies to outgoing and incoming trunks accessed through a trunk access code.

Other feature interaction

If an internal users call is redirected to EC500 (Extension to Cellular), DPT (Dial Plan Transparency), or IGAR (Inter-Gateway Alternate Routing) through a public trunk, then the internal user will not hear the warning tone.

Chapter 14: Allow direct input of Route Pattern for SIP station routing

The Allow direct input of Route Pattern for SIP station routing feature is introduced to simplify the routing configuration of a SIP station. This feature streamlines the traffic of a SIP station between Communication Manager and Avaya Aura® System Manager.

Detailed description of Allow direct input of Route Pattern for SIP station routing

This feature offers the following capabilities:

- Simplifies SIP station routing without using the additional AAR and ARS routing steps to select the route pattern for SIP station routing.
- Facilitates autosuggestion for route pattern mechanism on Session Manager.

Screens for administering Route Pattern enhancement for SIP station routing

Screen name	Purpose	Field
SIP Station	To set the trunk group value in the **SIP Trunk** field. The existing field value is upgraded with a prefix TG. For example, if a station has a SIP Trunk value set to 10 before the upgrade, the field is upgraded with a value TG10. To set the route pattern value in the **SIP Trunk** field. To assign a Route Pattern from RP1 to RP2000. Communication Manager allows a route pattern to be assigned as valid for the **SIP Trunk** field. RP prefixes the route pattern value.. For example, to assign route pattern 10 for SIP station routing, the SIP Trunk value is set to RP10. The existing options for the SIP Trunk field are not affected.	**SIP Trunk**
Stations with Off-PBX Telephone Integration	The trunk group value assigned to the **Trunk Selection** field is set with a prefix TG. The existing field value is upgraded with the prefix TG. For example, if a station has a SIP Trunk value set to 10 before the upgrade, the field is upgraded with the value TG10. Communication Manager allows a route pattern to be assigned as valid for the **Trunk Selection** field. RP prefixes the route pattern value. For example, to assign route pattern 10 for SIP station routing, the SIP Trunk value is set to RP10. The existing options for the **Trunk Selection** field are affected.	**Trunk Selection**

Table continues…

Screen name	Purpose	Field
Route Pattern	If used for SIP stations is set to `y`, Communication Manager automatically computes the primary and secondary Session Manager fields. Communication Manager computes these values by going through all the far end node names of signaling groups associated with all the SIP trunk groups on the station form. **Note:** Primary, secondary, third, and fourth Session Manager fields complement the System Manager feature to automatically suggest the route pattern on Communication Manager during add user form configuration. Avaya Aura® System Manager fetches all the route patterns having used for SIP stations value set to `y`. During the add user step, Avaya Aura® System Manager fetches matching route patterns for the given primary and secondary Session Manager servers.	**SIP Trunk**

Enabling Allow direct input of Route Pattern for SIP station routing

Procedure

1. Type `change route-pattern n`, where *n* is the route pattern number.
2. Set the value of the **Used for SIP stations** field to `y`.

   The system displays the following read-only fields:

   - Primary Session Manager
   - Secondary Session Manager
   - Third Session Manager
   - Fourth Session Manager

Chapter 15: Alphanumeric Dialing

Using the Alphanumeric Dialing feature you can enter an alphanumeric name to place data calls instead of a numeric string.

Detailed description of Alphanumeric Dialing

With Alphanumeric Dialing, a user can place a data call with Data Call Setup and an alphanumeric string or alpha-name for the call-destination address. For example, a user can type 9+1-800-telefon instead of 9+1-800-835-3366 to place a call. Users need to remember the alpha-name of the far-end terminating point.

With Alphanumeric Dialing, you can change a mapped string (digit-dialing address) without informing 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 name that the users enter is not in the table, the system denies the call attempt. The user receives an Invalid Address message (DCP) or a Wrong Address message (ISDN-BRI).

As data terminals use DCP or ISDN-BRI data modules to access the switch, dialing procedures vary:

- For DCP, at the `DIAL` prompt, users type the alphanumeric name and press `Enter`.
- For ISDN-BRI, at the `CMD` prompt, users type `d`, a space, the alphanumeric name, and press `Enter`.

Alphanumeric Dialing administration

Screens for administering Alphanumeric Dialing

Screen name	Purpose	Fields
Alphanumeric Dial Table	Map alphanumeric names to strings	• **Alpha-name** • **Mapped String**

Considerations for Alphanumeric Dialing

This section provides information about how the Alphanumeric Dialing feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Alphanumeric Dialing under all conditions. The following considerations apply to Alphanumeric Dialing:

- You cannot use Alphanumeric Dialing on telephones that have Hayes modems.
- More than one alphanumeric name can refer to the same digit string.

Chapter 16: Alphanumeric URI dialing

An alphanumeric URI consists of alphanumeric handles that are used to identify a directory number. In Communication Manager Release 7.1.3 onwards:

- You can assign alphanumeric URIs to hunt groups and vector directory numbers (VDNs).
- You can dial a hunt group and a VDN by using the SIP URI. When a call is made from a station to a hunt group or a VDN by using SIP URI, the call is sent to the respective hunt group or VDN.
- You can use alphanumeric handles for the following features:
  - Call forwarding
  - Priority calling
  - Whisper page
  - Directed call pickup
  - CPN block and unblock
  - Call unpark

Note:

To use alphanumeric URIs, you must configure the users with both the numeric handle and the alphanumeric handle in System Manager, and assign the numeric handle as Preferred in System Manager. For more information on configuring the users with alphanumeric URI dialing, see the description of **Preferred Handle** in the “New User Profile field descriptions” section in *Administering Avaya Aura® System Manager*.

Communication Manager Release 7.1.2 and later support placing and receiving calls by using alphanumeric URIs. Communication Manager supports alphanumeric handles on both SIP and H.323 deskphones.

Communication Manager supports the following format for an alphanumeric URI:

- <handle>@domain. For example, 123john@avaya.com

After you configure users with alphanumeric URI dialing, you can:

- Register users by using an alphanumeric handle.
- Place calls to an alphanumeric URI.

Limitations of alphanumeric URI dialing

Limitations of alphanumeric dialing is as follows:

- Alphanumeric URIs displayed on endpoints are truncated to 15 characters for incoming SIP trunk calls.

Chapter 17: Announcements

Use the Announcements feature to administer announcements that play for callers to your business. For example, you can inform callers that:

- The call cannot be completed as dialed.
- The call is in a queue.
- All lines are busy.

Announcements are often used in conjunction with music.

The source for announcements can be either integrated or external.

- Integrated announcements reside on an integrated VAL board, embedded in a gateway processor circuit pack, called a v VAL source throughout this feature description, and on Avaya Aura® Media Server.

  See Local announcements on gateways for a definition of v VAL.

- External announcements are stored on a separate piece of equipment called an adjunct and played back from the adjunct equipment.

Note:

This feature description uses the term announcement source to mean either integrated or external sources for announcements.

Related links

[Local announcements on gateways](#) on page 164

Detailed description of Announcements

Use the Announcements feature to play pre-recorded verbal messages to callers. You can also use announcements with music.

In Communication Manager 7.1.3 onwards, you can configure up to 9000 announcements for a single Avaya Aura® Media Server instance. Rest of the capacities around media announcement sources (MG/VAL board) remain unchanged.

For Communication Manager V11 or later, there are multiple telephone sessions. One session is associated with each active integrated announcement source. An announcement that is stored on an announcement source can play through any port on the announcement source.

Any announcement, except those announcements that are administered for “barge-in” (see Barge-in announcements), can play simultaneously through multiple ports. All ports can play the same announcement at the same time, and the system can connect multiple users to each of these announcements.

Audio files on the announcement source, gateway, or adjunct equipment can be grouped together based on two other features, Locally Sourced Announcements and Locally Sourced Music-on-Hold. For more information, see the “Locally Sourced Announcements and Music-on-Hold” feature.

The Announcements feature supports three general types of announcements:

- A delay announcement explains the reason for the delay and encourages the caller to wait.
- A forced announcement explains an emergency or a known service problem. Use a forced announcement when you anticipate numerous calls about a specific issue.
- An information announcement gives the caller instructions on how to proceed, information about the number called, or information that the caller might need.

Use the Announcements feature when:

- Direct Inward Dialing (DID) calls cannot be completed as dialed
- Incoming private-network-access calls cannot be completed as dialed
- Calls enter a split or a skill
- DDC, UCD, or direct-agent calls are in queue for an assigned interval
- ACD and Call Vectoring calls are in queue for an assigned interval
- The destination of a call is a recorded announcement extension
- The system routes a call to a vector that contains an announcement step
- An announcement extension is specified as a coverage point
- An announcement is the incoming destination of a trunk group
- The Hospitality Automatic Wakeup feature is in use

For information on music streaming from media server See chapter “Music streaming configuration” of the document *Implementing and Administering Avaya Aura® Media Server*.

Related links

Barge-in announcements on page 167

Voice Announcements over LAN

Voice Announcements over LAN (VAL), that use a TN2501AP integrated announcement circuit pack:

- Plays announcements over the time-division multiplexing (TDM) bus
- Has up to 1 hour of announcement storage time for each circuit pack
- Has 33 ports: 31 playback, 1 dedicated record, and 1 Ethernet

- Supports a 10/100 MB Ethernet interface for announcement and firmware file portability over a LAN by using file transfer protocol (FTP) server functions
- Supports generated `.wav` announcement files

Also, see local announcements on gateways.

Related links

Local announcements on gateways on page 164

VAL Manager

Avaya VAL Manager is a standalone application that you can use to copy announcement files and Communication Manager announcement information over a LAN connection. VAL Manager is part of the Avaya Integrated Management suite of products.

VAL Manager provides:

- Simplified administration for adding, changing, and removing Communication Manager announcement information.
- The ability to back up and restore announcement files and information to and from Communication Manager.
- The ability to view the status of announcements on the VAL announcement source.
- Also facilitates announcements to Avaya Aura® Media Server.

Announcements are stored in `.wav` files that can be sent to a voice announcement over a LAN announcement source without conversion. VAL Manager also provides a repository to back up and restore announcement files, and simplifies administration.

Over your LAN with VAL Manager, you can:

- View the current status of announcements
- Add, change, and remove announcements
- Copy and back up announcement files from S8300E, S8300D, and Avaya common servers to VAL Manager, and back.

Local announcements on gateways

Local announcements that are embedded in certain gateway processor circuit packs are known as virtual Voice Announcements over LAN (called “virtual VAL” or “v VAL”). Use VAL Manager to manage local announcements. Use v VAL for gateway embedded sources.

Local announcements (v VAL sources) are embedded in the following gateway processor circuit packs:

Gateway	Playback Channels	Total Announcement Time
G250	6	10 minutes

Table continues…

Gateway	Playback Channels	Total Announcement Time
G350	6	10 minutes
G700	15	20 minutes
G430	15	20 minutes
G450	63	45/240 minutes

Announcement devices and types

With the Announcements feature, you can administer either integrated announcements or announcements that are recorded on external devices. External devices connect to the server by means of analog-line media modules or auxiliary trunk interfaces.

The system stores integrated announcements on an integrated announcement source. The system can store multiple announcements on each announcement source up to the system capacity. The system can connect multiple users to each of these announcements.

Analog line announcement types

External announcement machines for recorded announcements can be interfaced using one of the analog line types. The external announcement machine can then be connected by an analog line port.

Analog

The analog announcement type provides an analog telephone interface using an analog line port for use with an announcement/audio source device that emulates analog telephones. The switch starts playback by applying ringing; the device indicates playback has stopped by going on-hook (opening the loop). The switch does not indicate to the device to stop playback. Use the analog type for announcements that play for a specific period and then go on-hook at the end. When the device goes on-hook to indicate that the playback ended, the caller listening to the announcement hears a click. (See DS1 announcement types, Auxiliary trunk announcement types, or Integrated announcement types for alternative types).

Analog-fd

Like the analog type, analog-fd provides an analog line interface and ringing starts the playback. However, a forward disconnect signal (open loop for about one-half second) is sent to the device to stop playback when there are no callers left to hear it.

Analog-m

Like the analog type, analog-m provides an analog line interface. However, ringing is not applied to start playback. Use this type for continuous playing music or audio sources. The device stays in an off-hook state when active and goes on-hook when it is not playing, is turned off, or is disconnected. This announcement type is used when the **Q** (queue) field is set to b to provide barge-in repeating or continuous-play announcements.

Related links

DS1 announcement types on page 166
Auxiliary trunk announcement types on page 166
Integrated announcement types on page 166

DS1 announcement types

The DS1 types provide analog-like interfaces with DS1 line ports, which are called Line Side DS1 or Line Side T1. Each of these types indicate to the announcement, music, or audio-source device to start playback using the Line Side T1 equivalent of ringing. The DS1 types also expect off-hook from the device to indicate that the playback is active and on-hook to indicate that the playback is inactive.

The ds1-id and ds1-sa types provide a forward disconnect using transitions of the A signaling bit to the device, which indicates when playback should be stopped. Callers listening to announcements do not hear clicks when the device disconnects (goes on-hook).

ds1-fd

The ds1-fd announcement type provides a TIA/EIA Foreign eXchange (FX) type DS1 interface. The forward disconnect signal is a toggle of the A bit from 0 to 1 and then back to 0 after 600 msecs. This type is used for Line Side T1 ports on the IVR system when they are used as an analog-like announcement device and is the recommended method for interfacing.

ds1-sa

The ds1-sa announcement type provides a TIA/EIA special-access type DS1 interface. The forward disconnect signal is a toggle of the A bit from 1 to 0 and then back to 1 after 600 msecs.

ds1-ops

The ds1-ops announcement type provides a TIA/EIA off-premises-station type DS1 interface that is used when the device does not support forward disconnect.

Auxiliary trunk announcement types

The Auxiliary Trunk announcement type supports an external announcement machine connected using a 4-wire auxiliary trunk interface, such as a 15A announcement system. The switch indicates to the device to start or stop the playback on the S lead; the device indicates that the playback is active on the S1 lead.

aux-trunk

Use the aux-trunk (auxiliary trunk) announcement type with a 4-wire interface external device when the playback is to be stopped and started by way of the S1 lead and S1 is used by the device to indicate playback started.

aux-trk-m

Use the aux-trk-m (auxiliary trunk music) with a 4-wire interface device for continuously playing music or audio sources that do not indicate that playback is active on the S1 lead. This announcement type is used when the **Q** field is set to b to provide barge-in repeating or continuous-play announcements

Integrated announcement types

The integrated announcement type stores announcements internally on the switch on an Integrated announcement source or embedded gateway processor equivalent. This can include a Branch Gateway VAL source, or Avaya Aura® Media Server.

The G700 v VAL source has 15 play ports, G350 and G250 v VAL source have 6 play ports, G430 v VAL source has 15 play ports, G450 v VAL source has 63 play ports, and the Avaya Aura® Media Server source is from M1 to M250. Integrated announcement sources are recommended for VDN of Origin Announcements and for other general and ACD announcement needs.

Based on the footprint, Avaya Aura® Media Server (MS)provides 1492 channels or 492 channels for VoIP. The channels are shared for announcements as well as calls.

integrated

Use the integrated announcement type for announcements that are stored on co-resident v VAL sources, or Avaya Aura® Media Server (MS). This announcement type is recommended for general, ACD, and vectoring announcements and for VDN of Origin Announcements.

integ-rep

The integ-rep (integrated-repeating) announcement type is used to provide integrated, repeating automatic wakeup announcements, and is implemented along with the multi-integ hospitality announcement type setting. This type can also be used for call center applications in vectoring where a continuous repeating announcement is required.

integ-mus

The integ-mus (integrated-music) announcement type is the same as the integ-rep type except that the **Q** field is set to b to provide a continuous repeating barge-in operation. This type is typically used to provide music on delay or on hold.

Any announcement that is stored on an announcement source can play through any port on the announcement source. Any announcement, except those announcements that are administered for “barge-in,” can play simultaneously through multiple ports. All 16 ports can play the same announcement simultaneously.

You must set the **Q** field to y on the Announcements/Audio Sources screen for each extension that you want to queue for integrated announcements. Integrated announcements queue only when all ports on the announcement source that contains the announcement are busy. The same queuing pool is used for all announcement sources. The system controls the announcement queue length for integrated announcements. However, you must set the queue length for analog or aux-trunk announcements.

Barge-in announcements

The system usually connects multiple callers to the beginning of an announcement, regardless of announcement type. However, you can also administer auxiliary trunk announcements, DS1 announcements, and integrated announcements to connect callers to hear a message that is already in progress. This capability is called “barge-in.”

Barge-in operation

When you administer barge-in by setting the **Q** field to b, only one port plays the announcement at any one time. When the system routes a call to that announcement, the call immediately connects to the port and the caller hears the announcement as it is playing.

Most administrators administer barge-in announcements to repeat continually while callers are connected to the port. In this way, the caller listens until the system plays the entire announcement.

Non-barge-in operation

If an announcement port is available when a call arrives, the system connects the call to the announcement starting from the beginning.

If an announcement port is unavailable and the announcement is administered with no as the queue option, the call does not enter the queue for the announcement and the caller hears busy or other feedback, depending upon how the announcement was accessed.

If an announcement port is unavailable and the announcement is administered with yes as the queue option, the call enters the announcement queue. When a port becomes available, the switch connects the calls waiting in the queue, up to the system limit, to the beginning of the announcement.

Announcement sources in the branch gateways

The Announcements feature provides a v VAL source for each branch gateway that is registered to either an S8300E, S8300D, or an Avaya duplex or Avaya simplex server. The duplex or simplex system supports 250 v VAL sources, and Avaya Aura® Media Server. S8300E and S8300D support 50 v VAL sources and Avaya Aura® Media Server (MS).

In Communication Manager 7.0 or later, the duplex or simplex system with the Increased Capacities Configuration supports 250 v VAL sources per system.

Note:

The software resources for integrated announcement sources and branch gateways are separated. The Branch Gateways v VAL sources are counted separately towards the limit of 50 on S8300E and S8300D, and 250 on the duplex or simplex system.

Announcement sessions

You can record, play back, or delete integrated announcements by initiating an announcement session. To do so, you must have console permissions assigned to your Class of Service (COS) for the internal station, or Remote Access barrier code to start an announcement session.

You can transfer to and from a computer, or delete announcement files over the LAN for the TN2501AP, H.248 v VAL, and Avaya Aura® Media Server sources by using the Voice Announcement Manager (VAM) software or an FTP client in conjunction with SAT commands.

Announcements for the VAL sources can also be recorded with a telephone using the procedures discussed in this section. Use those procedures to record announcements on the TN2501AP circuit packs, embedded v VAL sources on Branch Gateways, and Avaya Aura® Media Server.

Announcement recordings

After an end user accesses an announcement session, the user can dial 1 to record an announcement, 2 to play an announcement, or 3 to delete the announcement. If the announcement source memory is more than 90% full, then Communication Manager gives stutter dial tone when the user gains access to an announcement session. Even if the user hears stutter tone, the user should begin speaking to record the announcement.

Note:

You need to have a telephone or console with a class of service (COS) that provides console permissions to record announcements.

With VAL announcement sources, recording by telephone always uses a recording port that is dedicated for telephone access on the v VAL sources.

VAL announcement sources support recording announcements as PC `.wav` files, either on a local PC or made by a professional recording studio.

Note:

You cannot use a telephone to record an announcement with an audio group assignment.

For more information, see *Administering Avaya Aura® Communication Manager*.

Announcement session process

To begin an announcement session, the user must dial the administered Feature Access Code (FAC) followed by the announcement session.

- If an announcement session is already in progress, or if a save or restore command is in progress, then the user hears reorder tone (fast busy) and the system drops the call.
- If the telephone session port to an integrated announcement source is in use, then the user hears reorder tone followed by silence. This indicates that the port will be reserved for an announcement session. The user should redial the FAC and extension every 45 seconds to gain access to the port.

Note:

You need to have a telephone or console with a class of service (COS) that provides console permissions to record announcements.

You can have multiple telephone sessions, with one session associated with each active integrated announcement circuit pack.

Once a telephone user accesses an announcement session, the user can dial `1` to record an announcement, `2` to play an announcement, or `3` to delete an announcement. If the announcement source memory is more than 90% full, then the switch gives stutter dial tone when the user gains access to an announcement session. Even if the user hears stutter tone, the user can begin speaking to record the announcement.

Avaya recommends that you use a digital or IP telephone, since these telephones provide the best quality and functionality.

Tip:

Do not use remote telephone connections that route over IGAR (Inter-Gateway Alternate Routing)-supported facilities. The beginning portion of the recording, about four or five seconds, is not recorded after hearing the ready tone.

Locally sourced announcements and music overview

The Locally Sourced Announcement and Music feature is based on the concept of audio source groups. Using this feature, you can locate announcement and music sources on any or all the virtual VALs (v VAL) in a gateway. The v VAL circuit packs 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 the file that is assigned to the announcement extension.

For more information, see the feature description on “Locally Sourced Announcements and Music.”

Announcements administration

The following tasks are part of the administration process for the Announcements feature:

- Adding/changing/displaying or removing announcement extensions
- Setting up a gateway for announcements
- Recording and changing announcements
- Deleting and erasing announcements
- Setting up continuous-play announcements
- VAL announcements recording
- Converting announcement files to VAL format
- TTY announcement recording

Note:

The announcement boards must be busied out when adding or changing the announcement or audio-groups forms and announcements are not Avaya Aura Media Server.

Related links

TTY announcement recording on page 183
Converting announcement files to VAL format on page 180
Setting up continuous-play announcements on page 178
Recording and changing announcements on page 175
Setting up a gateway for announcements on page 174
Adding/changing/displaying or removing announcement extensions on page 172
Deleting and erasing announcements on page 177

VAL announcements recording on page 178

Screens for administering Announcements

Screen name	Purpose	Fields
Announcements/Audio Sources	Add, change, or delete individual announcement extensions, and the properties of the announcements. The announcement extension and file names must be defined before the announcement can be recorded using a telephone.	All
Integrated Announcements/Audio	List all existing announcement sources that have been administered.	All
Media-Gateway	Administer this screen to indicate that the gateway will be used as a v VAL source.	**V9** field set to gateway-announcements **Note:** These v VAL sources must also be enabled using the **enable announcement-board** command (see Setting up a media gateway for announcements on page 174).
Station	Set the Class of Service (COS) for the Announcements feature used for recording using a telephone.	**COS**
Feature Access Code (FAC)	Set up a Feature Access Code (FAC) to record announcements.	**Announcement Access Code**
Feature-Related System Parameters	Administer this screen if you plan to use Announcements with the feature that is associated with each field shown in the Fields column at right. Also used to set direct agent announcements.	• **DID/Tie/ISDN Intercept Treatment** • **Controlled Outward Restriction Intercept Treatment** • **Controlled Termination Restriction (Do Not Disturb)** • **Controlled Station-to-Station Restriction**

Table continues…

Screen name	Purpose	Fields
Hospitality	Administer this screen if you plan to use Announcements with the Hospitality feature.	• **Announcement Type** • **Length of Time to Remain Connected to Announcement**
Trunk Group	Administer this screen if you plan to use Announcements with the Trunk Group feature.	**Incoming Destination**
Coverage Path	Administer this screen if you plan to use Announcements with the Call Coverage feature.	**Coverage Points**
Hunt Group	Administer this screen if you plan to use Announcements with the Hunt Group feature.	• **First Announcement Extension** • **Second Announcement Extension**
Call Vector	Administer this screen if you plan to use Announcements with the Call Vectoring feature.	All fields that require announcements
VDN	Administer the VDN of Origin Announcement (VOA) extension.	**VDN of Origin Annc. Extension**

Adding/changing/displaying or removing announcement extensions

About this task

You need to assign an extension for each announcement that you want to record. After you define an announcement extension, you use the extension to record and access the announcement.

Note:

Announcement extensions and file names must first be defined before you can record announcements using a telephone.

Before you begin

To busy out the extension board, run `busyout board` <*board number*>.

Procedure

1. Enter `add announcement xxxx`.
2. In the **Extension** field, type the extension that you want to assign to this announcement.

   In the **Annc Name** field, type the unique name of the announcement that you are associating with the extension. If you use a gateway v VAL source, you must type a name, with no blank spaces, in the **Name** field. Do not type the file extension `.wav` in the **Name** field. This name becomes the unique file name for the announcement file. The system adds the `.wav` file extension to the name when the file is added to the announcement source.

For rules in naming files, see *Avaya Aura® Communication Manager Screen Reference*, the Announcements/Audio Sources screen, in *Administering Avaya Aura® Communication Manager*. Also see Announcement file format requirements.

3. In the **Annc Type** field, type the announcement type.

   See Announcement devices and types on page 165 for more information. If the Annc Type is integrated, you will see the related fields **Source** and **Protected**.

4. In the **COR** field, type the Class of Restriction that is associated with this announcement.
5. In the **TN** field, type the tenant partition, if any, that is associated with this announcement.

   Note:

   After the **Annc Name** field, the remaining fields may or may not appear, depending on the value that you typed in the **Annc Type** field.

6. In the **Queue** (queuing) field, perform one of the following actions:
   - Type `y` if you want calls to wait to hear an announcement when all the ports on the announcement source are busy. If the announcement is assigned to an audio group (see the “Locally Sourced Announcements and Music-on-Hold” feature), the system selects and plays the file in the closest announcement group.

     Important:

     Avaya recommends setting the **Queue** field to y for Call Center applications.

   - Type `n` if you do not want calls to wait to hear an announcement when all the ports on the announcement source are busy. If you type `n` in this field, a queue is not created, and the caller hears a busy signal or other feedback, depending on how the announcement was accessed.
7. The system displays `N/A` in the **Queue Length** field.

   You cannot change this field for integrated announcements. The length of the queue for integrated announcements is preset.

8. In the **Protected** field, perform one of the following actions:
   - Type `n` if you want to allow users with console permissions to change the announcement.
   - Type `y` if you do not want to allow users with console permissions to change the announcement. If you type `y` in this field, the announcement is protected and cannot be changed or overwritten by a new version of the file.
9. In the **Source** field, type one of the following values:
   - *ggg*`v9` for Branch Gateway v VAL sources, where *ggg* is the number of the gateway.
   - *mx* for Avaya Media Server, where *x* is the Avaya Media Server number.
   - *nn*, where *nn* equals 1-50 and is the audio group number of the locally-sourced announcement or locally-sourced Music-on-Hold group.

Note:

You can have numerous announcement and music-on-hold files, each assigned to a different extension, in a single audio group. For more information on audio groups, locally-sourced announcements, and locally-sourced music-on-hold, see the “Locally Sourced Announcements and Music-on-Hold” feature.

10. Repeat steps 2 through 8 with the correct information for each announcement you want to record.

    To get to the next screen, press `Next`.

11. Press `Enter` to save your changes.

Important:

These steps only create the administered extension and name for the announcement file. You fill the file space when you record an announcement.

Important:

If you want to change an announcement, use the command **`change announcement xxxx`**. To display announcements, type `display announcement xxxx`. To remove announcements, type `remove announcement xxxx`.

Note:

To administer DID Intercept announcements in a multi-location system where each location or city needs a different announcement, enter an audio group in the **Group/Port** field instead of a VAL port.

Related links

Announcement devices and types on page 165
Announcement file format requirements on page 179

Setting up a gateway for announcements

About this task

If you are going to use a Branch Gateways as a v VAL source, you must first set up the gateway to accept announcements.

Procedure

1. Enter `change media-gateway n`, where *n* is the number of the gateway.

   Note:

   If you need a list of the gateway numbers, enter **`list media-gateway`**. The system displays the Media-Gateway Report screen, listing all the gateways and their numbers.

2. Set the **V9** field to `gateway-announcements`.

Note:

There is no physical port named “V9” on Branch Gateways. The V9 port is virtual, and is used only for announcements.

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

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

Enabling the vVAL source announcement

Procedure

1. Type `enable announcement-board` *`ggg`*`V9`, where *ggg* is the number of the gateway in the Media Gateway screen. In this example, type `enable announcement-board 5V9`.
2. Select **Enter** to save your changes.

Note:

Use the gateway IP address as the v VAL address for FTP sessions.

Recording and changing announcements

About this task

You can use a system telephone or an attendant console to record a new announcement for callers to hear when callers dial a specific extension. Use the same procedure to change an existing announcement.

For recording VAL announcements, see Recording VAL announcements.

Related links

VAL announcements recording on page 178

Prerequisites

Procedure

1. Ensure that you have a telephone or an attendant console with a Class of Service (COS) that provides console permissions to record announcements.

   For more information on Class of Service, see the Class of Service feature.

2. Ensure that a Feature Access Code (FAC) has been set up to record announcements using a telephone.

   For more information on Feature Access Codes, see the Feature Access Code (FAC) feature.

3. Ensure that the necessary extensions, file names, and port addresses have been assigned using the Announcements/Audio Sources screen.

Recording or changing an announcement

Procedure

1. From a telephone or console, dial the Announcement Feature Access Code (FAC). For more information on FACs, see the Feature Access Code feature.
   - If you hear dial tone, continue with Step 2.
   - If you hear a fast busy signal, disconnect. Redial the FAC and the extension every 45 seconds until you hear dial tone.

   Note:

   You cannot record an announcement using a telephone for an extension with Locally Sourced Announcement/Music audio group (Gn) assigned. These files must be recorded using a PC. They can also be recorded to a single sourced extension using a telephone, then, using the FTP process, transferred to each of the sources in the audio group.
2. Dial the announcement extension.

   Do not enter the announcement session command until you hear dial tone. Enter # after the extension or wait for the dial tone to continue.
3. When you hear dial tone, dial 1 to begin recording.
   - If you hear a beep or a stutter tone, begin recording. If the integrated source memory becomes full while you are recording, the system drops your connection and does not retain the announcement.
   - If you hear intercept tone, disconnect. Record your announcement on another extension that is assigned to a different VAL circuit pack or v VAL source.
4. End the recording
   - If you are using a digital telephone, press #. You hear a dial tone again, and you can continue your session.
   - If you are using an analog telephone, disconnect quietly. If your analog telephone is not connected through lineside DS1, the system might record an electrical click at the end of the recording. You must redial the Announcement FAC to continue your session.
5. If you are using a digital telephone, and you want to listen to the announcement that you just recorded, dial 2. The recording plays back through the handset.
6. If you are not satisfied with the announcement, press:
   - to rerecord the announcement
   - to delete the announcement, and to end the recording session
7. To listen to the announcement after you disconnect, dial the announcement extension from any telephone or attendant console. The announcement plays through the handset.

   When you directly dial an announcement extension, for which an announcement has not been recorded, you hear silence instead of a busy tone with the VAL-type sources, such as the v VAL source.

Note:

You must wait 15 seconds after you record an announcement before you can dial the extension to hear the announcement replay. During this 15-second window, you cannot record a new announcement, and no one can play this announcement. However, you can rerecord the announcement during this 15-second period. To rerecord the announcement, dial the Announcement FAC, dial the extension, and then press 1 before the 15-second timer expires.

Deleting and erasing announcements

Before you begin

- Look up the announcement extension, which is mapped to a specific announcement source by location.
  - On the SAT screen, type `list integrated-annc-boards`.
  - Determine the extension for the announcement that you want to delete.
- Write down the Feature Access Code (FAC) for an announcement session.

  For more information on FACs, see the Feature Access Code feature.

About this task

You can use a system telephone or an attendant console to delete recorded announcements from an integrated announcement source.

Note:

The system denies any attempt to delete an announcement while it is playing, being transferred, or backed up to FLASH (amber LED is flashing), regardless of whether the attempt is from a system telephone, the SAT.

Procedure

1. From a telephone or an attendant console, dial the Announcement FAC.
2. When you hear dial tone, dial the announcement extension.
3. When you hear dial tone, dial `3` to delete the announcement. You hear a confirmation tone. If the announcement is protected or is playing at the time you perform this step, you hear a fast busy signal (the reorder tone), and the system does not delete the announcement.
4. Disconnect the telephone.
5. To ensure that an announcement was deleted, dial the extension of the deleted announcement. If the announcement was deleted, you hear a busy signal.
6. Repeat Steps 1 through 5 for each announcement that you want to delete. You can delete only one announcement at a time.

Deleting an announcement extension

Procedure

1. Type `change announcements`. Press `Enter`.

   The system displays the Announcements/Audio Sources screen.
2. Delete the information in the **Ext**, **Name**, and **Type** fields.
3. Press `Enter` to save your changes.

Erasing an announcement source

Procedure

1. Type `erase announcements` *n*, where *n* is the address of the announcement source that contains the announcement that you want to erase.

   The system displays a warning message that confirms the deletion.
2. Press `Enter` to erase the announcements on the announcement source.

Setting up continuous-play announcements

About this task

You can set up announcements to continuously repeat while callers are connected to the announcement, so that a caller can listen until the system plays the entire announcement. With a “barge-in” queue, you do not need a separate port for each announcement.

For example, you can set up an Automatic Wakeup announcement to repeat, and use a barge-in queue. When guests pick up the telephone to hear an announcement at a particular time, they use only one port. The message repeats on that port until the last guest goes off-hook and the message ends.

Procedure

1. Type `change announcements`. Press `Enter`.

   The system displays the Announcements/Audio Sources screen.
2. In the **Q** field, type `b` on the same line as the extension for the announcement.
3. Leave the name that is in the **Name** field, or enter a new description for the announcement.
4. Press `Enter` to save your changes.

VAL announcements recording

You can record an announcement for callers to hear when the callers dial a specific extension, or as part of call vectoring. Use the same steps to change an existing announcement.

You can record announcements at a:

- Professional recording studio

- Computer
- System telephone

Preparing to record VAL announcements

About this task

You must complete the following actions before you can record VAL announcements:

Procedure

Ensure that the announcement administration is complete.

You must assign a name to the file before you can record an announcement. For more information, see Adding/changing/displaying or removing announcement extensions.

Related links

Adding/changing/displaying or removing announcement extensions on page 172
Viewing the Event Report for announcement events on page 184

Announcement file format requirements

To be compatible with the gateway v VAL source and Communication Manager, announcement recordings must have the following parameters:

- CCITT A-Law or CCITT μ-Law compression format. Do not use PCM.
- 8-KHz sample rate
- 8-bit resolution (bits per sample)
- Mono (channels = 1)
- The μ-Law compression format is used in the United States, and A-Law compression format is used internationally. Use the compression format that is specified on the Location Parameters screen.
- Filenames for the VAL announcement sources cannot contain blank spaces, nor any of the following characters:
  - Period (.)
  - Comma (,)
  - Colon (:)
  - Asterisk (*)
  - Question mark (?)
  - Less than (<)
  - Greater than (>)
  - Forward slash (/)
  - Backward slash (\)

  The filename itself is case sensitive, but the file extension `.wav` must be lowercase. Announcements that are recorded in this format occupy 8-KB per second of file space for

each second of recorded speech. For example, a 10-second announcement creates an 80-KB `.wav` file.

Do not type the `.wav` file extension for the file name in the Announcements/Audio Sources screen. The system does not display the `.wav` file extension on this screen.

Recording a VAL announcement at a computer

Procedure

1. At the computer, open the application that you use to record `.wav` files, such as Microsoft Sound Recorder.
2. Set the recording parameters.
3. Speak into a microphone that is connected to the computer and record the announcement.
4. Assign a name to the `.wav` file, following the rules for defining announcement names on the Announcements/Audio Sources screen.

   Make sure that the resulting file name on the PC does have the `.wav` file extension as part of the name.

   Important:

   For the system to access this announcement file, the file name, minus the `.wav` file extension, must exactly match the name on the Announcements/Audio Sources screen.
5. Play the announcement back at the computer before you transfer the file to the announcement source.

Related links

Recording and changing announcements on page 175

Converting announcement files to VAL format

About this task

If you share recordings in a multisite environment with Communication Manager and Avaya Interactive Voice Response (IVR) systems, you can convert announcement files for use on either system. If you want to convert an announcement file to the required format, you can use a sound recording utility application, such as Microsoft Sound Recorder.

Procedure

1. Open the sound recording application on your computer.

   For example, you might use Microsoft Windows Sound Recorder.
2. Open the file that you want to convert.
3. Check the file properties to determine if you must change the parameters.
4. If you must change the recording parameters, look for a conversion tool.

Some tools have a Convert Now option. Other tools, for example, Microsoft Sound Recorder, are included with the Save As function.

5. Change the file parameters to parameters that are listed in Announcement file format requirements.

Note:

In some applications, assigning the format (for example, CCITTμ-Law) sets the remainder of the default parameters. Check each parameter carefully, and change the default setting to match the required parameters if necessary. Note that CCITT μ-Law or A-Law can be referred to as ITU G.711 μ-Law or ITU G.711 A-Law, respectively.

Related links

Announcement file format requirements on page 179

Converting announcements for Interactive Voice Response

About this task

The Interactive Voice Response (IVR) system has a recording conversion utility that supports file formats that are similar to the formats that VAL requires. However, the conversion utility can read only PCM-format announcement files.

Procedure

1. If the companding format of the file is already PCM, go to Step 5.

   If you are unsure what the file format is, continue with Step 2.
2. At a computer, open the sound recording application.
3. Open the file that you want to convert.
4. Save the announcement (Convert Now or Save As) with these parameters:
   - Format: PCM
   - Bits/Sample: 8
   - Sample Rate: 8-KHz
   - Mono (channels = 1)

Note:

The recording conversion utility requires that announcement files be in PCM format. VAL files must be in CCIT A-Law or μ-Law format.

5. Open the file in the recording conversion utility.
6. Convert the file to SSP format.

VAL announcement deletions

Preparing to delete VAL announcements

Procedure

1. Look up the announcement information.

   Type `list directory board`. Press `Enter`.

2. Determine which announcements you want to delete, either by extension or file name.
3. Decide whether you are:
   - Using The SAT to delete individual VAL announcement files
   - Using The SAT to delete all VAL announcements on a circuit pack
   - Deleting and erasing announcements

   Note:

   The system denies any attempt to delete an announcement while the announcement is playing, being transferred, or backed up to Flash memory.

Related links

Using the SAT to delete individual VAL announcement files on page 182
Using the SAT to delete all VAL announcements on a circuit pack on page 182
Deleting and erasing announcements on page 177

Using the SAT to delete individual VAL announcement files

Procedure

Enter `remove file board board-location /annc/`*`filename.wav`*, where *`filename.wav`* is the name of the file that you want to delete.

Note:

File names are case sensitive, and require the `.wav` file extension.

The `/annc` portion of the command directs the system to the announcement subdirectory on the announcement source. The `/closed.wav` portion indicates to delete the file `closed.wav`.

Using the SAT to delete all VAL announcements on a circuit pack

Procedure

1. Type `busyout board` *`board-location`*, where *board-location* is the 5-character number that is assigned to the circuit pack. Press `Enter`.

Note:

When the VAL circuit pack is busied out,

- Announcements on that circuit pack cannot play.

2. Type `erase announcements board` *`board-location`*, where *board-location* is the 5-character number that is assigned to the circuit pack. Press `Enter`.

Caution:

This command deletes the specified announcement file in both RAM and Flash memory. The circuit pack firmware ignores the protect flag (**Pro** field) when you erase the announcement files.

3. Type `list directory board`. Press `Enter`.
4. Verify that no files are listed.

Note:

The announcement directory on the v VAL source is `/annc`.

5. Type `list integrated-annc-boards`. Press `Enter`.

Check the list. The **Length in Seconds** field shows `0` if the announcement was deleted.

Setting up v VAL

About this task

A virtual VAL (v VAL) source uses the IP address of the gateway. Type `list media-gateway` to find this IP address. Make sure that the v VAL is administered, and that the **V9** field on the Media Gateway screen is administered and enabled.

TTY announcement recording

Record announcements for Teletypewriter device (TTY) callers in the same way as you record voice announcements. However, instead of recording from the handset of your telephone, you record from a TTY device. You can use an acoustic coupler into which you place the telephone handset to attach the device to your telephone, or plug the TTY device directly into the back of a digital telephone. After you call the announcement extension, and press `1` to record, you type the announcement into the TTY device.

If you use an acoustic coupler to connect your telephone for recording, you can record TTY and voice into a single announcement. In this case, after you press 1 to record, you can type the TTY message, and then immediately pick up the handset to record the voice message. For this type of recording, digital telephones also offer the option to press # to complete the recording, which eliminates any extraneous noise at the end of the recording. Unfortunately, this method for combined TTY and voice recordings is to create extraneous noise in the middle of your announcements.

An efficient alternative to record with your telephone is to create `.wav` files on other recording applications, such as a PC, and then copy and save the `.wav` files to your announcement source. In this case, the announcement files must meet the same criteria as voice recordings. See Announcement file format requirements for more information.

Related links

Announcement file format requirements on page 179

Reports for Announcements

The following reports provide information about the Announcements feature:

- Event Report

  If a working VAL announcement file is deleted the next attempt to play the announcement fails, and the system adds a software event to the Event Report. You can view the Event Report to see if the announcement was deleted, and to see if other events occurred that are related to announcements.

  For information on how to access this report, see Viewing the Event Report for announcement events

- Voice Announcement Measurements

  You can view a report of announcement measurements. This report includes how many times an announcement was queued to play, how many callers dropped while in the queue, and how many times all announcement ports were busy during the report period.

  For information on how to access this report, see Viewing Voice Announcement Measures.

Related links

Viewing the Event Report for announcement events on page 184
Viewing Voice Announcement Measures on page 185

Viewing the Event Report for announcement events

About this task

If a working announcement file is deleted, the next attempt to play the announcement fails, and the system adds a software event to the Event Report. You can view this log to see if the announcement has been deleted, and to see if other events have occurred related to announcements.

Procedure

1. Type `display events`. Press `Enter`.

   The system displays the Event Report input screen. This input screen helps you focus the report on events of a certain type or from a certain time.

2. In the **Category** field, select or type `denial`.
3. You can further limit the report by setting the **Interval** field to one of the following selections (select from the help list or type the first letter):
   - all
   - month
   - day
   - hour
   - minute
4. Press `Enter`.

   The system displays the Events Report screen for the parameters that you set.
5. Look at the 2027 entry in the **Event Type** field.
   - The **Event Description** field explains that the announcement is not on the announcement source.
   - The **Event Data 1** field contains the announcement number (hexadecimal in the lower three digits).

     The Events Report displays the denial event only once.

Viewing Voice Announcement Measures

About this task

You can view the Voice Announcement Measurements report, including how many times an announcement was queued to play, how many callers dropped while in queue, and how many times all announcement ports were busy during a specified period.

Procedure

Enter `list measurements announcements all today-peak`.

For detailed information on these reports and the associated commands, see *Avaya Aura® Communication Manager Reports*.

Interactions for Announcements

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

Automatic Call Distribution (ACD)

Recorded announcements are used extensively for ACD, Call Vectoring, Call Prompting, Expert Agent Selection (EAS), Vector Directory Number (VDN) of Origin Announcement, Direct

Department Calling, and Uniform Call distribution (UCD) features. See the individual features for interaction details.

Automatic Wakeup

If you use an integrated, multiple-integrated, or external type of announcement for Automatic Wakeup, you can also administer the announcement to repeat and to enable *barge-in* as a queue type. The benefit of repeating announcements and *barge-in* queues is that you do not need a separate port for each wakeup announcement. When guests go off-hook to receive an announcement at a particular time, the guests use only one port. The message repeats on the port until the last guest goes off-hook, and the message ends.

Announcements troubleshooting

This section lists the known or common problems that users might experience with the Announcements feature.

Problem	Possible cause	Action
No sound or poor sound quality.	Bad file format.	Ensure that the file formats are compatible. A good announcement file format must have the following parameters: • 8-Kbps sample rate • 8-bit resolution (bits per sample) • A-law or μ-Law companding format • Mono (channels = 1)
	Incorrect companding mode.	Ensure that the same companding mode is administered on page 1 of the Location Parameters screen (type `change location- parameters`) for both environments.
An announcement does not play.	If a working VAL announcement file is deleted, the next attempt to play the announcement fails, and the system adds a software event to the Denial Events Log.	View the Denial Events log to determine if the announcement was deleted. If the announcement was deleted, restore or rerecord the announcement.
The system displays error code E28 when you attempt to restore announcements.	An integrated announcement source is not installed in the system.	Install an integrated announcement source.

Table continues…

Problem	Possible cause	Action
The system displays error code E31 when you attempt to restore announcements.	A call is connected to the announcement on the announcement source and the port is busy.	Wait for the call to disconnect, and try to restore announcements again. If the system has an abnormal shutdown, or if there is a processor interchange during the restore announcements process, the restore process fails. There is no valid announcement on the announcement source. Repeat the process when the system is operating properly.

Announcement capacities and load balancing

Understanding how Communication Manager handles announcements helps with questions of load-balancing announcement traffic. Communication Manager supports up to 3,000 announcements across the enterprise. Each of as many as 10 integrated announcement circuit packs, H.248 gateway virtual VAL source, and Avaya Aura® Media Server is limited to 256 announcements.

You can have up to 250 virtual VAL sources per system, and Avaya Aura® Media Server (MS).

Each Virtual VAL source has 64 playback ports (with 20 minutes storage capacity). Initially, each caller that is to hear a non-barge-in announcement on that source is connected to an available port until each port has one caller connected. Initially,64 callers can be hearing an announcement from a single virtual VAL source. The same announcement can be playing from multiple ports, each starting at a different time. Once all ports are busy playing announcements, subsequent callers that are to hear an announcement residing on that circuit pack/source are queued for that source.

Communication Manager queue size over all integrated announcement sources is 4,000 callers (duplex and simplex servers/S8300E or S8300D server). When a port becomes available, all callers (up to 1,000) waiting in the queue for a specific announcement on that source are connected to the available port to hear the announcement play from the beginning on a first-in, first-out basis.

The **`measurements announcements`** command can be used to monitor the system and help determine burst conditions, providing efficient load balancing of the traffic.

Chapter 18: Attendant Auto Start and Don’t Split

Using the Attendant Auto Start and Don’t Split features an attendant can press any key on the keypad to start a call without the need to first press the `Start` button. If the attendant is on an active call and presses digits on the keypad, the system automatically splits the call and dials the second call.

The Don’t Split feature deactivates the Auto Start feature, and the system sends touch tones over the line.

Detailed description of Attendant Auto Start and Don’t Split

Auto Start and Don’t Split are two features that work together. These two features reduce the number of buttons that attendants must press to handle calls.

Auto Start

If the attendant is on a call and presses any key on the keypad, the system automatically splits the current call, places the call on hold, and dials the next call. The system disables the **Start** button, and stops support for end-to-end signaling..

To extend a current call to another extension, the attendant dials the extension. The system automatically places the current call on hold. Once the called party answers, the attendant presses the **Release** button to extend the call.

Don’t Split

To deactivate the Auto Start feature and not split a current call, the attendant presses the **Don’t Split** button. One use of the Don’t Split feature is to send touch tones to pick up answering machine messages. When the Don’t Split feature is active, parties on the call hear the keys that the attendant presses.

To reactivate the Auto Start feature and restart end-to-end signaling, the attendant can:

- Press the `Don’t Split` button again.

- Press `Cancel`.
- Allow the current call to terminate

Attendant Auto Start and Don't Split administration

The following task is a part of the Attendant Auto Start and Don't Split feature:

- Assigning a Don't Split button

Related links

Assigning a Don’t Split button on page 189

Preparing to administer Attendant Auto Start and Don't Split

Procedure

Ensure that you set up the attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Auto Start and Don’t Split

Screen name	Purpose	Fields
Attendant Console	Assign a **Don’t Split** button.	Any unassigned button in the **Feature Button Assignments** area.

Assigning a Don’t Split button

Procedure

1. Type `change attendant n`, where *n* is the number of the attendant console. Press `Enter`.
2. On the Attendant Console screen, click `Next` until you see the **Feature Button Assignments** area.
3. In the **Feature Button Assignments** area, assign `dont-split` to an available button.
4. Press `Enter` to save your changes.

Considerations for Attendant Auto Start and Don’t Split

This section provides information about how the Attendant Auto Start and Don’t Split features behave in certain circumstances. Use this information to ensure that you receive the maximum

benefits of Attendant Auto Start and Don’t Split under all conditions. The following considerations apply to Attendant Auto Start and Don’t Split:

- If an attendant activates Auto Start, and then dials an Automatic Alternate Routing (AAR) number where the values in the **min** and the **max** fields in the AAR Analysis Table are unequal, the attendant must press the pound key (#) after the digit string. If the attendant does not press the pound key, the system does not process the call.

Interactions for Attendant Auto Start and Don’t Split

This section provides information about how the Attendant Auto Start and Don’t Split features interact with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Auto Start and Don’t Split in any feature configuration.

Call Detail Recording (CDR) Account Code Dialing

If the system is using Call Detail Recording Account Code Dialing, the Auto Start and the Don’t Split features are not activated.

Visually Impaired Service (VIS)

If VIS is activated or deactivated while Don’t Split is active, the system automatically deactivates the Don’t Split feature.

Chapter 19: Attendant Auto-Manual Splitting

Using the Attendant Auto-Manual Splitting feature, an attendant can announce an incoming call to a user without being heard by the calling party. The attendant can also use the Attendant Auto-Manual Splitting feature to consult privately with the called party without being heard by the calling party.

Detailed description of Attendant Auto-Manual Splitting

Using the Attendant Auto-Manual Splitting feature, the attendant can split the calling party away from a conversation. The attendant can then confidentially determine if the called party wants to accept the call.

The system automatically activates the Attendant Auto-Manual Splitting feature when the attendant, who is active on a call, presses any of the following buttons:

- Start
- An extension
- Any Hundreds Select button plus an extension
- Trunk Group Select

Attendant Auto-Manual Splitting administration

The system activates the Attendant Auto-Manual Splitting feature when you set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

This section describes the prerequisites and the screens for the Attendant Auto-Manual Splitting feature.

Screens for administering Attendant Auto-Manual Splitting

Screen name	Purpose	Fields
Attendant Console	Set up an attendant console.	All

Chapter 20: Attendant Backup

Using the Attendant Backup feature, you can give access to attendant console features from specially administered backup telephones, and you can answer calls promptly, thus providing efficient service to your callers.

When the attendant console is busy, you can answer overflow calls from the backup telephones by pressing a button or dialing a Feature Access Code (FAC). You can then process the calls as if you are at the attendant console.

You can assign the Attendant Backup feature to only multi-appearance telephones. Avaya recommends the following multi-appearance telephone models as a backup for the attendant:

- Avaya 9408 Digital Deskphone
- Avaya 9408 Digital Deskphone with SBM24 button module
- Avaya 9608 IP Deskphone
- Avaya 9608 IP Deskphone with BM12 button module
- Avaya 9608 IP Deskphone with SBM24 button module

Detailed description of Attendant Backup

You can configure your system to have backup telephones for the attendant. With the Attendant Backup feature, designated users can answer calls that the attendant cannot immediately answer. These designated users can also provide some of the services that the attendant usually provides.

Designated users can access some attendant console features from the backup telephones when the:

- Queue of received calls reaches one of the following administered warning levels:
  - Number of calls in the queue
  - Time that a particular call has been in the queue
- Attendant console is in Night Service

A user with console permissions can:

- Activate Automatic Wakeup for another extension
- Activate and deactivate controlled restrictions for another extension, or a group of extensions

- Activate and deactivate Do Not Disturb for another extension, or a group of extensions
- Activate Call Forwarding for another extension
- Add and remove agent skills
- Record integrated announcements

To assign the Attendant Backup capabilities, you use **Console Permissions** field on the Class of Service screen.

Attendant Backup Alerting

The Attendant Backup Alerting feature notifies the backup telephones that the attendant needs assistance to handle calls. The system provides both audible and visual alerting to backup telephones when the calls in the attendant queue reach the administered warning levels. When the queue drops below the administered warning level, alerting stops.

Audible alerting also occurs when the attendant console is in Night Service, regardless of the size of the attendant queue.

Once the system alerts the backup telephones, designated users can answer an attendant call by:

- Pressing the `atd-qcalls` button
- Dialing the Feature Access Code (FAC) for Trunk Answer Any Station (TAAS) feature.

Attendant Backup administration

The following task is part of the administration process for the Attendant Backup feature:

- Setting up Attendant Backup telephones

Related links

Setting up Attendant Backup telephones on page 195

Preparing to administer Attendant Backup

Procedure

1. Assign a Class of Service (COS) value to the multiappearance telephones that you use for Attendant Backup.

   On the Class of Service screen, you must set the **Client Room** field to `n`, and the **Console Permissions** field to `y`.

   For more information, see the Considerations for Attendant Backup, as well as the Class of Service feature.

2. On the Feature Access Code (FAC) screen, type a FAC in the **Trunk Answer Any Station** field.

Then share the FAC with each of the attendant backup users. For more information, see the Feature Access Code feature.

3. Set up the attendant console.

   For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Backup

Screen name	Purpose	Fields
Class of Service	Ensure that the Attendant Backup feature is set up correctly.	**Client Room**
	Assign console permissions to the backup telephones.	**Console Permissions**
Console Parameters	Administer the Attendant Backup Alerting feature.	**Backup Alerting**
	Set the queue warning parameters.	• **Calls in Queue Warning** • **Time in Queue Warning (sec)**
Feature Access Code (FAC)	Assign a FAC for backup telephone users.	**Trunk Answer Any Station**
Station	Assign an `atd-qcalls` feature button for backup telephone users.	Any available button field in the **Feature Button Assignments** area.

Setting up Attendant Backup telephones

Procedure

1. Configure your system.
2. Define Class of Service console permissions.
3. Assign console permissions to backup telephones.
4. Train designated users.

Related links

Configuring your system for Attendant Backup on page 195
Defining Class of Service console permissions on page 196
Assigning console permissions to backup telephones on page 196
Attendant Backup user training on page 197

Configuring your system for Attendant Backup

Procedure

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

The system displays the Console Parameters screen.

2. In the **Backup Alerting** field, type `y`.

   The system can now notify any telephone that has an **atd-qcalls** feature button when the:

   - Attendant queue reaches the warning level
   - Console is in night service

3. In the **Calls in Queue Warning** field, type the maximum number of calls that can be in the attendant queue before the system alerts the backup telephones.
4. Click `Next` until you see the **Time in Queue Warning (sec)** field.
5. In the **Time in Queue Warning (sec)** field, type the maximum number of seconds that a caller can be in the attendant queue before the system alerts the backup telephones.
6. Press `Enter` to save your changes.

Defining Class of Service console permissions

Procedure

1. Type `change cos`. Press `Enter`.

   The system displays the Class of Service screen.

2. In the **Console Permissions** row, change `n` to `y` in a numbered column.

   Each column is a COS identification number.

3. To assign any other permissions for this COS, change `n` to `y` in the corresponding column.
4. Press `Enter` to save your changes.

Assigning console permissions to backup telephones

Procedure

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

   The system displays the Station screen.

2. In the **COS** field, assign the COS that you created for the console permissions.
3. Click `Next` until you see the **Feature Button Assignments** area.
4. In the **Feature Button Assignments** area, assign `atd-qcalls` to an available button.

   The **atd-qcalls** button provides visual alerting for this telephone. When the **atd-qcalls** button:

   - Is dark, the attendant queue contains no calls
   - Shows a steady light, the attendant queue contains calls.
   - Shows a flashing light, the number of calls in the attendant queue exceeds the limit that you set for the queue. At this point, the backup telephone user also hears an alert signal.

5. Press `Enter` to save your changes.
6. Repeat this process for each backup telephone.

Attendant Backup user training

You must train the backup users. The backup users must know:

- How to interpret the **atd-qcalls** button lights
- If the telephones of the backup users do not have an **atd-qcalls** button, the FAC for the TAAS feature
- Your procedure for how to answer attendant calls
- Your procedure for how to transfer attendant calls

End-user procedures for Attendant Backup

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Answering Attendant Backup calls

About this task

If the **atd-qcalls** button on your telephone is flashing, the number of calls in the attendant queue exceeds the maximum limit. You also hear an alert signal every 10 seconds.

Procedure

To answer the call, either:

- Press the `atd-qcalls` button on your telephone.
- Dial the FAC for the TASS feature.

Considerations for Attendant Backup

This section provides information about how the Attendant Backup feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Backup under all conditions. The following considerations apply to Attendant Backup:

- Backup telephone users must meet the following criteria to answer alerting calls in the attendant queue:
  - Have a multiappearance telephone

- Have an **atd-qcalls** feature button assigned to the telephone
- Be assigned a Class of Service (COS) that has the **Client Room** COS field set to n. Classes of Service are defined on the Class of Service screen.

  If the **Client Room** COS field is set to y, the user receives intercept treatment when the user tries to use the Attendant Backup feature.

- When the attendant console is in day mode and the Attendant Backup feature is disabled, backup telephone users do not hear the audible alert signal. Backup telephone users also cannot dial the Feature Access Code (FAC) for Trunk Answer Any Station (TAAS) to answer attendant calls.

Interactions for Attendant Backup

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

Ringer Cutoff

Activating the Ringer Cutoff feature disables the audible alerting signal. If a backup telephone has Ringer Cutoff activated, the system audibly alerts the telephone only when the attendant queue exceeds the queue warning level.

If Ringer Cutoff is not activated, the system audibly alerts the backup telephone every 10 seconds until the attendant queue falls below the queue warning level.

Trunk Answer Any Station (TAAS)

If the system is in night mode and a TAAS port is unassigned, backup telephone users must dial the Feature Access Code (FAC) for Trunk Answer Any Station (TAAS) to answer queued calls.

Tenant Partitioning

You cannot use the Attendant Backup feature if Tenant Partitioning is enabled.

Chapter 21: Attendant Call Waiting

Using the Attendant Call Waiting feature, an attendant can notify a single-line telephone user, who is on an existing call, that another call is waiting. Once the attendant notifies the user, the attendant can answer other calls.

Detailed description of Attendant Call Waiting

The system automatically activates the Attendant Call Waiting feature whenever an attendant originates or extends a call to a single-line telephone user who is on an existing call. When the system activates Attendant Call Waiting, the:

- Attendant hears a call waiting ringback tone
- Telephone user hears a call waiting tone
- Calling party does not hear a tone

The attendant can place a call in progress on hold. After the attendant answers the call on hold, the attendant can use the Hold button to return to the held call. The attendant can alternate between the two calls.

For example, assume that extension 123, a single-line telephone, is busy. An attendant extends an incoming call to extension 123. The attendant hears the call waiting ringback tone, which indicates that Attendant Call Waiting is activated. The attendant can:

- Announce the call-waiting condition to the calling party
- Cancel the Attendant Call Waiting feature, and ask the calling party to call again later
- Release the caller, or place the call on hold at the console

  Releasing an attendant-originated call drops the call completely.

The user at extension 123 hears a call-waiting tone, and knows that a call is waiting. The user can:

- Terminate the existing call
- Place the existing call on hold, and answer the waiting call

If the user does not answer the waiting call before a preassigned time interval, the system returns the call to the attendant.

Attendant Call Waiting administration

The system activates the Attendant Call Waiting feature when you set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

The following tasks are part of the administration process for the Attendant Call Waiting feature:

- Setting up single-line telephones
- Changing the call-waiting signal
- Modifying timed intervals

Related links

Setting up single-line telephones for Attendant Call Waiting on page 200
Changing the call-waiting signal on page 201
Modifying timed intervals for Attendant Call Waiting on page 201

Screens for administering Attendant Call Waiting

Screen name	Purpose	Fields
Station	Send calls to busy single-line telephones	**Att. Call Waiting Indication**
Feature-Related System Parameters	Change the call-waiting signal	**Attendant Originated Calls**
Console Parameters	Indicate the maximum number of seconds that a call can remain on hold before the system alerts the attendant	**Timed Reminder on Hold**
	Indicate the maximum number of seconds that a call can remain on hold before the call returns to the attendant	**Return Call Timeout**

Setting up single-line telephones for Attendant Call Waiting

Procedure

1. Type **change station *n***, where *n* is the single-line extension that you want to change. Press `Enter`.
2. On the Station screen, click `Next` until you see the **Att. Call Waiting Indication** field.
3. Set the **Att. Call Waiting Indication** field to `y`.
4. Press `Enter` to save your changes.
5. Repeat this process for each single-line telephone on your system.

Changing the call-waiting signal

About this task

You can change the number of alerting tones (1, 2, or 3 beeps) that the user hears when the attendant extends a call. You can set the number of tones to indicate an internal call, an external call, and a priority call. The system defaults are:

- Internal: 1
- External: 2
- Priority: 3

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. On the Feature-Related System Parameters screen, click `Next` until you see the **Distinctive Audible Alerting** area.

   Note:

   The Feature-Related System Parameters screen displays the **Distinctive Audible Alerting** field only when the **Tenant Partitioning** field on the System Parameters Customer Options screen is set to `n`. If the **Tenant Partitioning** field is set to `y`, you must change the **Distinctive Audible Alerting** area on the Tenant screen.
3. Change the number of tones (1, 2, or 3 beeps) that a user hears when the system activates the Attendant Call Waiting feature.

   If you change one field, **Internal**, **External**, or **Priority**, Avaya recommends that you change all fields. A user then knows what kind of call the attendant is extending.
4. Press `Enter` to save your changes.

Modifying timed intervals for Attendant Call Waiting

About this task

If either the Timed Reminder on Hold interval, or the Return Call Timeout interval, expires before the call is answered, the call returns to the attendant console.

Procedure

1. Type **change console-parameters**. Press `Enter`.
2. On the Console Parameters screen, click `Next` until you see the **Timed Reminder on Hold** field and the **Return Call Timeout** field.
3. In the **Timed Reminder on Hold** field, type the maximum number of seconds that a call can remain on hold before the system alerts the attendant.
4. In the **Return Call Timeout** field, type the maximum number of seconds that a call can remain on hold before the call returns to the attendant.

Note:

You must allow at least 5 seconds for each ring at all points in a coverage path. This time ensures that the entire calling path is completed before the system returns the call to the console.

5. Press `Enter` to save your changes.

Considerations for Attendant Call Waiting

This section provides information about how the Attendant Call Waiting feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Call Waiting under all conditions. The following considerations apply to Attendant Call Waiting:

- Attendant Call Waiting applies only to calls that are made to single-line telephones within the system.
- Only one call can wait at a time.

Interactions for Attendant Call Waiting

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

Automatic Callback

Activating Automatic Callback at the called telephone denies Attendant Call Waiting.

Call Coverage

The system redirects Attendant Call Waiting calls to coverage if the called telephone has Data Privacy or Data Restriction activated. The system redirects the call to coverage if all three of the following conditions are met:

- The Data Privacy or Data Restriction feature is activated
- You assign call coverage to a telephone
- The user activates Send All Calls, or coverage criteria is met
  - The Coverage Don’t Answer interval specifies how long that call remains directed to the called telephone before the system redirects the call to coverage. If Attendant Call Waiting is applicable on the call, the feature is active for the duration of the Don’t Answer interval only. At the end of this interval, the system redirects the call to coverage.
  - If the Return Call Timeout (Timed Reminder) interval expires before the Don’t Answer interval expires, the call does not go to coverage, but returns to the attendant console. If the Don’t Answer interval expires first, the system redirects the call to coverage. The

system can still return the call to the attendant console if a coverage point does not answer the call before the Return Call Timeout expires.

- If the **Station Hunting** field is assigned, and the called telephone is busy, the system redirects the call to the Hunt To Station Assignment value.
- If Send All Calls is active, or if the redirection criterion is Cover All Calls, the system immediately redirects the call to coverage instead of to Attendant Call Waiting.
- An attendant can release an extended call at any point during the call with no affect on the preceding operations.

Data Privacy and Data Restriction

Activating Data Privacy or Data Restriction at the called telephone denies Attendant Call Waiting.

Direct Department Calling (DDC) and Uniform Call Distribution (UCD)

Calls to a DDC group or to a UCD group do not wait. However, calls can enter the group queue, if a queue is provided.

Loudspeaker Paging

Activating Loudspeaker Paging at the called telephone denies Attendant Call Waiting.

Music-on-Hold Access

If the call is a trunk-transferred call that is administered to receive Music-on-Hold, the calling party hears music. Otherwise, the calling party hears ringing.

Recorded Telephone Dictation Access

Activating Recorded Telephone Dictation Access at the called telephone denies Attendant Call Waiting.

Chapter 22: Attendant Calling of Inward Restricted Stations

Using the Attendant Calling of Inward Restricted Stations feature, an attendant can override an inward restriction Class of Restriction (COR).

Detailed description of Attendant Calling of Inward Restricted Stations

A telephone that is restricted from receiving inbound calls cannot receive public network, attendant-originated, or attendant-extended calls. Using the Attendant Calling of Inward Restricted Stations feature, the attendant can override this restriction.

Attendant Calling of Inward Restricted Stations administration

The following task is part of the administration process for the Attendant Calling of Inward Restricted Stations feature:

- Setting up Class of Restriction override

Related links

Setting up Class of Restriction override for the attendant on page 205

Preparing to administer Attendant Calling of Inward Restricted Stations

Procedure

Set up the attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Calling of Inward Restricted Stations

Screen name	Purpose	Fields
Class of Restriction	Override any Class of Restriction that is assigned to a telephone.	**Restriction Override**

Setting up Class of Restriction override for the attendant

Procedure

In the Class of Restriction screen, set the **Restriction Override** field to `attendant`.

For more information, see the Class of Restriction feature.

Chapter 23: Attendant Conference

Using the Attendant Conference feature, an attendant can set up a conference call for as many as six parties, including the attendant. However, if the **12–party Conferences** field is enabled in the Feature-Related System Parameters screen, 12 parties can participate in a conference call. In an active call involving a desk attendant or an Avaya one-X® Attendant, only the attendant can initiate a conference call or transfer the call to another party. Communication Manager blocks other parties from initiating a conference call or transferring the call.

Detailed description of Attendant Conference

The Attendant Conference feature allows an attendant to set up a conference call for as many as six parties, including the attendant. However, if the **12–party Conferences** field is enabled in the Feature-Related System Parameters screen, 12 parties can participate in a conference call.

To set up a conference call by using a desk attendant, the attendant dials the number of a conferee, and then presses the **Split** button to add a conferee.

To set up a conference by using one-X® attendant, the attendant clicks the **Transfer** button, selects the new party, and then clicks the **Recall** button.

Administering Attendant Conference

The system activates the Attendant Conference feature when you set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

The following task is part of the administration process for the Attendant Conference feature:

- Setting up Attendant Conference.

Related links

Setting up Attendant Conference on page 207

Screens for administering Attendant Conference

Screen name	Purpose	Fields
Feature-Related System-Parameters	Set up the Attendant Conference feature.	• **Public Network Trunks on Conference Call** • **Conference Parties with Public Network Trunks** • **Conference Parties without Public Network Trunks**

Setting up Attendant Conference

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. On page 6 of the Feature-Related System-Parameters screen, in the **Public Network Trunks on Conference Call** field, type a number between 0 to 5, or 11.

   Note:

   If you set the **Public Network Trunks on Conference Call** field to `0`, the system does not display the **Conference Parties with Public Network Trunks** field.
3. In the **Conference Parties with Public Network Trunks** field, type a number between 3 to 6, or 12.
4. In the **Conference Parties without Public Network Trunks** field, type a number between 3 to 6, or 12.
5. Save the changes.

Considerations for Attendant Conference

- The attendant can set up only one conference call at a time. The attendant can hold or release the conference call only by using the attendant console.
- The attendant cannot handle other calls while the attendant sets up a conference call.
- If the attendant is one of the conferees in a conference call, only the attendant can add a new party to the call.

Interactions for Attendant Conference

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

Bridged Call Appearance

A user can press the **Bridged Appearance** button on the telephone and join a conference call only if no more than five parties are on the call.

Call Vectoring

A vector directory number (VDN) can be included as a party in a conference call only after vector processing terminates for that call. Vector processing terminates, for example, after a successful route-to command.

Trunk-to-Trunk Transfer

If Trunk-to-Trunk Transfer is disabled on the Feature-Related System-Parameters screen, and the attendant releases from a conference call that involves only trunk conferees, the system disconnects the trunks.

When a user of a BRI, digital, or hybrid multifunction telephone dials enough digits to route a call that might otherwise be routed differently if the user dials additional digits, the telephone does not recognize the **Conference** or the **Transfer** buttons. For the system to recognize the **Conference** or the **Transfer** buttons, the user must either dial the number again after 3 seconds or dial the pound key (**#**) at the end of the dialed string at the end of the dialed string. The system identifies this action to route the call and not wait for the additional digits. The system then completes the call.

Attendant conferencing might not operate properly if the central office (CO) does not provide answer supervision. In this case, you must set the **Answer Supervision Timeout** and the **Outgoing End of Dial** fields to the same nonzero number and the **Receive Answer Supervision** field to n.

If the CO provides answer supervision, you can set the **Answer Supervision Timeout** field to 0 and the **Receive Answer Supervision** field to y.

Chapter 24: Attendant Control of Trunk Group Access

Use the Attendant Control of Trunk Group Access feature to allow the attendant to control outgoing and two-way trunk groups. The attendant usually activates this feature during periods of high use. This is helpful when an attendant wants to prevent telephone users from calling out on a specific trunk group. Some reasons are to reserve a trunk group for incoming calls or for a very important outgoing call.

This feature also prevents telephone users from directly accessing an outgoing trunk group that the attendant has controlled.

Detailed description of Attendant Control of Trunk Group Access

When an administered threshold for a trunk group is reached, a warning lamp for that trunk group lights on the attendant console. The attendant can then access control of that trunk group. To gain direct access to an outgoing trunk group, the attendant presses the button that is assigned to that trunk group.

When the Attendant Control of Trunk Group Access feature is activated:

- Internal callers who use a trunk access code to dial out are connected to the attendant
- The attendant can prioritize outgoing calls for the remaining trunks

The system processes Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) route pattern calls without the need for attendant control.

Each attendant console has 12 designated Trunk Hundreds Select buttons. These buttons can be administered for the Attendant Control of Trunk Group Access feature. You can also administer each console with up to 12 feature buttons for Trunk Hundreds Select buttons, which gives you up to 24 buttons to use for this feature.

The Each Trunk Hundreds Select button has a busy lamp. The busy lamp is ON when the members of the trunk group are busy.

Note:

If you administer one of the two-lamp feature buttons on a basic console as a Trunk Hundreds Select button, use the bottom lamp as the busy lamp.

The Trunk Hundreds Select buttons have the following two additional lamps for Attendant Control of Trunk Group Access:

- Warn (warning) lamp

  The warning lamp lights when the administered number of trunks are busy in the associated trunk group. You administer the **Busy Threshold** field on the associated Trunk Group screen to determine when to light this warning lamp.

- Cont (control) lamp

  The control lamp lights when the attendant activates the Attendant Control of Trunk Group Access feature for the associated trunk group. You can assign the **act-tr-grp** and **deact-tr-g** buttons on the Attendant Console screen to activate and deactivate the trunk group access.

Attendant Control of Trunk Group Access administration

The following tasks are part of the administration process for the Attendant Control of Trunk Group Access feature:

- Setting The trunk group threshold
- Assigning Attendant Control of Trunk Group Access buttons

Related links

Setting the trunk group busy threshold on page 211
Assigning Attendant Control of Trunk Group Access buttons on page 211

Preparing to administer Attendant Control of Trunk Group Access

Procedure

Set up the attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Control of Trunk Group Access

Screen name	Purpose	Fields
Trunk Group	Determine the threshold for when to light the warning lamp	**Busy Threshold**
Attendant Console	Assign buttons to activate and deactivate trunk group access	Any unassigned buttons in the **Feature Button Assignments** area.

Setting the trunk group busy threshold

Procedure

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

   The system displays the Trunk Group screen.

2. In the **Busy Threshold** field, type the number of trunks that must be busy to light the warning lamp on the attendant console.

   The range is from 1 to 255.

   For example, a trunk group contains 30 trunks. If you want to alert the attendant when 25 or more trunks are in use, type `25`.

3. Press `Enter` to save your changes.

Assigning Attendant Control of Trunk Group Access buttons

Procedure

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

   The system displays the Attendant Console screen.

2. Click `Next` until you see the **Feature Button Assignments** area.

3. In the **Feature Button Assignments** area, assign `act-tr-grp` and `deact-tr-g` to two available buttons.

4. Press `Enter` to save your changes.

Interactions for Attendant Control of Trunk Group Access

This section provides information about how the Attendant Control of Trunk Group Access feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Control of Trunk Group Access in any feature configuration.

Authorization Codes

Authorization codes do not collect when a trunk group has an incoming destination set to the attendant.

Automatic Route Selection (ARS) and Automatic Alternate Routing (AAR)

Activating Attendant Control of Trunk Group Access removes the controlled trunk groups from the ARS and the AAR patterns. Deactivating the feature reinserts the groups into the patterns. The system does not route ARS calls to the attendant.

QSIG

QSIG trunks do not support Attendant Control of Trunk Group Access.

Uniform Dial Plan (UDP)

Activating Attendant Control of Trunk Group Access removes the controlled trunk groups from preferences. Deactivate this feature for the UDP to access trunk groups.

Chapter 25: Attendant Direct Extension Selection

Using the Attendant Direct Extension Selection (DXS), you can track the idle or busy status of an extension and place or extend calls to extensions without dialing the extension.

The Attendant DXS feature is sometimes referred to as the Attendant Direct Extension Selection with Busy Lamp Field feature.

Detailed description of Attendant Direct Extension Selection

With Attendant DXS, you can use either Standard or Enhanced DXS Tracking:

- Standard DXS Tracking

  If your attendant console has one or more Hundreds Select buttons, the attendant can press both a Hundreds Select button and a DXS button to access an extension.

- Enhanced DXS Tracking

  Use Enhanced DXS Tracking if your attendant console:

  - Does not use Hundreds Select buttons
  - Uses Hundreds Select buttons, but you have one or more hundreds groups that are not administered by a Hundreds Select button

    To access an extension, the attendant can:

  - Press a Group Select button
  - Dial the first 2 or 3 digits of the extension
  - Press the DXS button to access an extension

When the system tracks a group of extensions, the attendant can press the DXS button to place or extend subsequent calls to extensions in that group without the need to reselect the group. Whether the attendant uses a Hundreds Select button or the Group Select button, both capabilities eliminate the need to dial extensions.

Extensions might be telephones, hunt-group extensions, off-switch extensions such as uniform dial plan (UDP) extensions, or other extensions.

Whichever method you use to access and track DXS extensions, you can use a Group Display feature button to view the group of extensions that are currently being tracked. This button on the console indicates the range of extensions that the selector console is tracking.

Note:

An associated DXS lamp for a vector directory number (VDN) is always dark. The attendant can use the DXS button to place a call to a VDN.

Attendant DXS supports the following capabilities:

- Standard DXS Tracking
- Enhanced DXS Tracking

Related links

Standard DXS Tracking on page 214
Enhanced DXS Tracking on page 214

Standard DXS Tracking

The basic selector console has 8 Hundreds Select buttons, and 100 DXS buttons. The enhanced selector console has 20 Hundreds Select buttons, and 100 DXS buttons. You can assign 12 additional Hundreds Select buttons to feature buttons on the attendant console.

The total number of Hundreds Select buttons for each attendant, including both attendant console feature buttons and selector console buttons, cannot exceed 20.

Enhanced DXS Tracking

Enhanced DXS Tracking is helpful if you have more than 100 telephones, but use a console that does not have Hundreds Select buttons administered. Enhanced DXS Tracking is also helpful if you have more telephones than Hundreds Select buttons, and thus have hundreds groups that are administered with Hundreds Select buttons.

To use Enhanced DXS, assign a **Group Select** button on the Attendant Console screen. The attendant uses this button to track and extend calls to telephones that do not have associated Hundreds Select buttons. You cannot use Enhanced DXS Tracking if your extensions have fewer than 3 digits.

Group Display button for DXS tracking

You can administer a **Group Display** button on the Attendant Console screen to help the attendant track extension status. When the attendant presses this button, the system displays the range of extensions that are currently tracked by the selector console. Administer the **Group Display** button for either the feature area or the display area of the console.

If the attendant presses this button, the system identifies the digits that are associated with a Hundreds Select button. If no Hundreds Select button is lit, the system identifies the digits that were last entered with the **Group Select** button. The system continues to track the selected group of extensions until the attendant selects a new group of extensions.

Attendant Direct Extension Selection administration

The following tasks are part of the Attendant Direct Extension Selection feature:

Preparing to administer Attendant Direct Extension Selection

Procedure

Set up the attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Direct Extension Selection

Screen name	Purpose	Fields
Attendant Console	Assign a DXS button.	Any available button field in the **Hundreds Select Button Assignments** area

Considerations for Attendant Direct Extension Selection

This section provides information about how the Attendant Direct Extension Selection (DXS) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Direct Extension Selection (DXS) under all conditions. The following considerations apply to Attendant Direct Extension Selection (DXS):

- With this feature, the attendant can place calls to:
  - 800 extensions with the basic selector console
  - 2,000 extensions with the enhanced selector console
  - Up to 99,999 extensions with the Group Select feature button (extension numbers from 100 to 99,999)

  If the attendant is tracking a hundreds group with either a Hundreds Select button or the Group Select feature button, the attendant presses the DXS button to access an extension.
- This feature provides the attendant with a visual indication of the idle or busy status of the extensions that are assigned to the selected hundreds group. You can simultaneously monitor up to 100 extensions for idle or busy status.
- Enhanced DXS Tracking does not support extensions with fewer than 3 digits.
- Extension tracking is possible only for the system on which the attendant resides.

Interactions for Attendant Direct Extension Selection

This section provides information about how the Attendant Direct Extension Selection (DXS) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Direct Extension Selection (DXS) in any feature configuration.

Attendant Display

When the attendant uses the Attendant Direct Extension Selection with Busy Lamp Field, the alphanumeric display identifies the call through the Attendant Display.

Call Coverage

If Send All Calls is activated, or if the Call Coverage redirection criteria are met, the system redirects an extended call to the coverage path.

Centralized Attendant Service (CAS)

When the attendant uses a DXS button to make a CAS call, the attendant hears ringback tone after a few seconds.

Chapter 26: Attendant Direct Trunk Group Selection

You can use the Attendant Direct Trunk Group Selection feature to directly access an idle outgoing trunk. With this feature, the attendant gets directs access to an idle outgoing trunk when the attendant presses the button that is assigned to the trunk group. This feature eliminates the need for the attendant to memorize, or look up, and dial the trunk access codes (TACs) that are associated with frequently used trunk groups.

Detailed description of Attendant Direct Trunk Group Selection

You can use up to 12 designated Trunk Hundreds Select buttons on each console. You can also administer up to 12 of the feature buttons as additional Trunk Hundreds Select buttons, for a total of 24 Trunk Hundreds Select buttons per console. You can use each button to directly access an outgoing select trunk group.

While an attendant talks on a call, the attendant can be split away that call and place a new call to the outgoing trunk that is specified by the trunk group select button. The attendant can then press **Release** to connect the split-away parties to the dial tone on the trunk. Or the attendant can dial the destination, and press **Release** to connect the split-away party to the called party.

All Trunk Hundreds Select buttons, including any that are administered on the feature buttons, have a Busy lamp. This lamp lights when all trunks in the associated trunk group are busy. If you administer one of the two-lamp feature buttons on a basic console as a Trunk Hundreds Select button, use the bottom lamp as the Busy lamp. Six of the designated buttons on a basic console, or all 12 designated buttons on an enhanced console also have a Warning lamp and a Control lamp. The Warning lamp lights when a preset number of trunks in the associated trunk group are busy. The Control lamp lights when the attendant activates Attendant Control of Trunk Group Access for the associated trunk group.

You can assign Loudspeaker Paging zones instead of trunk groups to Trunk Hundreds Select buttons. The Busy lamp then indicates the idle or the busy status of the associated Loudspeaker Paging zone.

Attendant Direct Trunk Group Selection administration

This section describes the prerequisites and the screens for the Attendant Direct Trunk Group Selection feature.

Preparing to administer Attendant Direct Trunk Group Selection

Procedure

Set up the attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Direct Trunk Group Selection

Screen name	Purpose	Fields
Attendant Console	Assign trunk access codes (TACs) for local and remote systems.	Any available button field in the **Direct Trunk Group Select Button Assignments** (Trunk Access Codes) area

Considerations for Attendant Direct Trunk Group Selection

This section provides information about how the Attendant Direct Trunk Group Selection feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Direct Trunk Group Selection under all conditions. The following considerations apply to Attendant Direct Trunk Group Selection:

- Attendant Direct Trunk Group Selection eliminates the need for the attendant to memorize, or look up, and dial a trunk access code (TAC) that is associated with frequently used trunk groups. A label that is associated with each Trunk Hundreds Select button identifies the destination or use of the button. For example, buttons might be labeled Chicago, FX, or WATS. The attendant presses the button to select an idle trunk in the required group.

Interactions for Attendant Direct Trunk Group Selection

This section provides information about how the Attendant Direct Trunk Group Selection feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Direct Trunk Group Selection in any feature configuration.

Attendant Control of Trunk Group Access

If Attendant Control of Trunk Group Access is provided, the Attendant Direct Trunk Group Selection feature must also be provided.

QSIG

Attendant Direct Trunk Group Selection does not apply to QSIG trunks.

Chapter 27: Attendant Intrusion

Using the Attendant Intrusion feature, an attendant can intrude on an existing call. The Attendant Intrusion feature is also called Call Offer.

Detailed description of Attendant Intrusion

The attendant uses the Attendant Intrusion feature to announce a new call or a message to a user who is already on a call.

When the attendant releases the call of the user, the source party either waits at the analog telephone of the user, or holds on an available line appearance on a digital telephone.

Note:

Only one call can be waiting at a time. If a call is already waiting on the telephone of the intruded party, the source party, once split from the attendant, cannot also wait.

Attendant Intrusion administration

The following task is part of the administration process for the Attendant Intrusion feature:

- Assigning an intrusion button

Related links

Assigning an intrusion button on page 221

Preparing to administer Attendant Intrusion

Procedure

Set up the attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Intrusion

Screen name	Purpose	Fields
Attendant Console	Assign an **intrusion** button	Any unassigned button in the **Feature Button Assignments** area

Assigning an intrusion button

Procedure

1. Type `change attendant n`, where *n* is the number of the attendant console. Press `Enter`.
2. On the Attendant Console screen, click `Next` until you see the **Feature Button Assignments** area.
3. In the **Feature Button Assignments** area, assign `intrusion` to an available button.

   In this example, we assign `intrusion` to button 5.
4. Press `Enter` to save your changes.

Interactions for Attendant Intrusion

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

- Intrusion is denied in when a:
  - Telephone is on a conference call with the administered maximum number of conferees
  - Call is established with Data Privacy activated
  - Call is established with Data Restriction activated
  - Telephone is a forward-to point of another telephone
  - Telephone is busy talking to another attendant
- If a call is already waiting for an intruded party, the second caller, who is split from the attendant, cannot use Call Waiting to wait for the intruded party. The attendant display shows “wait” or “busy”. If an intrusion is possible, the attendant display shows “1 wait” or “1 busy”.
- In Italy only, the system provides Attendant Intrusion on remote telephones through TGU/TGE trunks.

Chapter 28: Attendant Lockout - Privacy

Use the Attendant Lockout - Privacy feature to prevent an attendant, who drops from a multiparty conference call, from reentering the call. The attendant can be recalled only by a telephone user who is on the multiparty call.

You administer this feature on a system-wide basis. The Attendant Lockout - Privacy feature is either activated or deactivated.

Detailed description of Attendant Lockout - Privacy

The Attendant Lockout - Privacy feature provides privacy for parties on a multiparty call. The parties can hold a private conversation without interruption by the attendant. The multiparty call must be held on the attendant console.

Attendant Lockout - Privacy administration

The following task is part of the administration process for the Attendant Lockout - Privacy feature:

- Activating or deactivating the Attendant Lockout - Privacy feature

Related links

Activating or deactivating the Attendant Lockout - Privacy feature on page 223

Preparing to administer Attendant Lockout - Privacy

Procedure

Set up the attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Lockout - Privacy

Screen name	Purpose	Fields
Console Parameters	Activate or deactivate the Attendant Lockout - Privacy feature.	Attendant Lockout

Activating or deactivating the Attendant Lockout - Privacy feature

Procedure

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

   The system displays the Console Parameters screen.
2. In the **Attendant Lockout** field, perform one of the following actions:
   - Type `y` to activate this feature.
   - Type `n` to deactivate this feature.
3. Press `Enter` to save your changes.

   For more information, see *Administering Avaya Aura® Communication Manager*.

Interactions for Attendant Lockout - Privacy

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

Attendant Recall

If Attendant Lockout - Privacy is activated, use Attendant Recall if you must recall the attendant.

Individual Attendant Access

Attendant Lockout - Privacy applies only to attendant group calls. This feature does not affect individual attendant calls.

Trunk-to-Trunk Transfer

Attendant Lockout - Privacy does not function when a call that uses Trunk-to-Trunk Transfer is held on the console.

Chapter 29: Attendant Override of Diversion Features

Using Attendant Override of Diversion Features, the attendant can bypass an active call-diverting feature. Such features include Send All Calls, Call Coverage, and Call Forwarding. An attendant can use this feature, in combination with Attendant Intrusion, to place an emergency call or an urgent call to a user.

Attendant Override of Diversion Features administration

This section contains prerequisites and the screens for administering the Attendant Override of Diversion Features feature.

Preparing to administer Attendant Override of Diversion Features

Procedure

Set up an attendant console.

For information on how to set up an attendant console, see the *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Override of Diversion Features

Screen name	Purpose	Fields
Attendant Console	Administer the **Attendant Override** button.	Any available button field in the **Feature Button Assignments** area.

Chapter 30: Attendant Priority Queue

Use the Attendant Priority Queue feature to place incoming calls to an attendant, that cannot be immediately answered, into an ordered queue. With this feature, you can define 13 different categories of incoming attendant calls. Emergency calls always have the highest priority.

Detailed description of Attendant Priority Queue

When an attendant cannot immediately answer calls, the system can place incoming calls into categories, or into a call type within a category.

With Attendant Priority Queue, attendants can answer calls by call category, such as trunk type. Attendant Priority Queue places incoming calls in a queue:

- According to the priority levels that you assign for each type of call
- In order of time stamp within each level

The calling party hears ringback until an attendant answers the call.

Attendant Priority Queue supports the following capabilities:

- Priority by Call Category
- Priority by Call Type

Related links

Attendant queue priority by call category on page 225
Attendant queue priority by call type on page 227

Attendant queue priority by call category

Assign an Attendant Priority Queue level to each of 13 incoming attendant call categories. Each category has a default level. You can reset the priority level for any category.

Important:

Retain the priority level for Emergency Access calls. Emergency Access calls must remain priority 1.

The attendant call categories are:

- Emergency Access. Calls from users who dial the emergency access code. The default is the highest priority level. This category must remain priority 1.

- Assistance Call. Calls from users who:
  - Dial the attendant group access code
  - Have the Manual Originating Line Service feature activated
- CO Call. Incoming central office (CO), foreign exchange (FX), or Wide Area Telecommunications Service (WATS) trunk calls to an attendant group. This category excludes trunk calls that are returned to the attendant group after a timeout or a deferred attendant recall.
- DID to Attendant. Incoming direct inward dial (DID) trunk calls to an attendant group.
- Tie Call. Incoming Tie trunk calls, including dial-repeating and direct types.
- Redirected DID Call. DID or Automatic Call Distribution (ACD) calls that time out, and are rerouted to the attendant group. The timeout can be caused by:
  - Ring/no-answer
  - Busy condition
  - Number Unobtainable
- Redirected Call. Calls that are assigned to one attendant, but redirected to the attendant group because the attendant is now busy.
- Return Call. Calls that are returned to the attendant after the calls time out. If the attendant is now busy, calls are redirected to the attendant group.
- Serial Call. Calls from the Attendant Serial Call feature. Calls fit this category when an outside trunk call, that the attendant designates as a serial call, is extended to and completed at a telephone, and then the user goes on-hook. If the attendant who extends the call is busy, the system redirects the call to the attendant group.
- Individual Attendant Access. Calls from users, incoming trunks, or a system feature, to the Individual Attendant Access (IAA) extension of a specific attendant. If the attendant is busy, the call remains in a queue until the attendant is available.
- Interpositional. Calls from one attendant to the Individual Attendant Access (IAA) extension of another attendant.
- VIP Wakeup Reminder Call. Call from the Hospitality feature that send a wake-up reminder to the attendant to call the room.
- Miscellaneous Calls. All other calls.

You can assign the same priority level to more than one category. Assigning all categories the same priority level creates a first-in first-out queue.

When the Attendant Priority Queue displays at least one call, the Calls Waiting lamp lights steadily on all active attendant consoles. If the number of calls in the queue reaches the calls-waiting threshold for the attendant group, the Queue Warning lamp lights steadily on all active attendant consoles.

Attendant queue priority by call type

You can further define the priority that you assign to calls in the Attendant Priority Queue by call type. Then, within each call type, you can prioritize calls by time.

The call types, in descending order of priority, are:

- Type 1 calls are outgoing public network calls that receive answer supervision when the Answer Supervision Timer of the trunk group expires, even if the trunk is still ringing. Type 1 calls are also incoming calls that the attendant answers.
- Type 2 calls are incoming external public network calls before the calls receive answer supervision, or before the Answer Supervision Timer of the trunk group expires.
- Type 3 calls are all other calls, which include internal calls, conference calls, and tie-trunk calls of any type.

Note:

External public network calls have priority over all other calls, including conference calls. Answered public network calls have priority over calls that are not yet answered.

Attendant Priority Queue administration

The following tasks are part of the administration process for the Attendant Priority Queue feature:

- Setting attendant queue category priorities
- Setting the number of calls in the attendant queue
- Call type button assignment
- Translating the Call Type button into a user-defined language

Related links

Setting attendant queue category priorities on page 228
Setting the number of calls in the attendant queue on page 228
Translating the Call Type button into a user-defined language on page 229
Call type button assignment on page 229

Preparing to administer Attendant Priority Queue

Procedure

Set up the attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Priority Queue

Screen name	Purpose	Fields
Console Parameters	Assign priorities to queue categories.	All fields in the **Queue Priorities** area
Feature-Related System Parameters	Set the number of calls in the queue.	Reserved Slots for Attendant Priority Queue
Attendant Console	Assign a **Call Type** button.	Any unassigned button in the **Feature Button Assignments** area
Language Translations	Translate the **Call Type** button into a user-defined language.	Call Type

Setting attendant queue category priorities

Procedure

1. Type `change console-parameters`. Press `Enter`
2. On the Console Parameters screen, click `Next` until you see the **Queue Priorities** area.
3. Type a number from 1 to 13 next to each category.

   This number indicates the priority of the category. The number 1 indicates the highest priority. The number 13 indicates the lowest priority.
4. In the field, perform one of the following actions:
   - If you want to order calls by call type within each category, type `y`.
   - If you do not want to order calls by call type within each category, type `n`.
5. Press `Enter` to save your changes.

Setting the number of calls in the attendant queue

Procedure

1. Type **change system-parameters features**. Press `Enter`.
2. On the Feature-Related System Parameters screen, click `Next` until you see the **Reserved Slots for Attendant Priority Queue** field.
3. In the **Reserved Slots for Attendant Priority Queue** field, type a number between 2 and 75.

   This number indicates how many nonemergency calls can go into the priority queue. The default is 5.
4. In the **Number of Emergency Calls Allowed in Attendant Queue** field, type a number between 0 and 75.

   This number indicates how many emergency calls can go into the priority queue. The default is 5.

5. Press `Enter` to save your changes.

Call type button assignment

You can assign a **Call Type** button on the attendant console. When you press this button, the system displays the call type of the active call. For more information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Translating the Call Type button into a user-defined language

About this task

If you use a user-defined language to display messages on the attendant console, you can translate the **Call Type** button.

Procedure

1. Type `change display-messages miscellaneous-features`. Press `Enter`.
2. On the Language Translations screen, click `Next` until you see the **English: Call Type** field.
3. In the **English: Call Type** field, translate the button label into the user-defined language.
4. Press `Enter` to save your changes.

Considerations for Attendant Priority Queue

This section provides information about how the Attendant Priority Queue feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Priority Queue under all conditions. The following considerations apply to Attendant Priority Queue:

- An incoming call that defaults to an attendant and is then redirected to the attendant group, does not change the associated Attendant Priority Queue level. The reason code that the system displays on the answering attendant console remains the same as the reason code that the system displays on the original attendant console.

Interactions for Attendant Priority Queue

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

Multiparty Calls

The system always treats multiparty calls as Type 3 calls. If a multiparty call becomes a single-party call while in the queue, the multiparty call remains a Type 3 call.

Night Service-Hunt Group

When you use Night Service-Hunt Groups, retrieve calls from the hunt groups instead of from the Attendant Priority Queue. Since call-type prioritization does not apply to hunt groups, do not retrieve calls in order of call type, unless you designate the Attendant Priority Queue as the termination.

Off-Premises Station

The system always identifies calls from off-premises telephones as Type 3 calls.

Chapter 31: Attendant Recall

Using the Attendant Recall feature, a user can recall the attendant while the user is on a call.

- Single-line users press the recall button or flash the switchhook to recall the attendant.
- Multi-appearance users press the conference or transfer button to recall the attendant and remain on the connection when either button is used.

Detailed description of Attendant Recall

With the Attendant Recall feature, users can call the attendant for assistance while the users are currently on a call. Users can activate the Attendant Recall feature only when the users are on a:

- Two-party call
- Conference call that is held at the attendant console

Attendant Recall administration

The system activates the Attendant Recall feature when you set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

This section describes the prerequisites and the screens for the Attendant Recall feature.

Screens for administering Attendant Recall

Screen name	Purpose	Fields
Attendant Console	Set up an attendant console	All

End-user procedures for Attendant Recall

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

To recall the attendant:

- Single-line users press the recall button or flash the switchhook.
- Multiappearance users press the conference button or the transfer button.

Interactions for Attendant Recall

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

Individual Attendant Access

If a user is holding a hunt-group call to an individual attendant, the user who is active on the call cannot recall the attendant. However, the user can transfer calls, and make conference calls.

Chapter 32: Attendant Room Status

Using Attendant Room Status, the attendant can see a room's occupancy state and housekeeping status.

Note:

This feature is available only if you have **Enhanced Hospitality** enabled and have the **DXS lamp** field on the console. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to Attendant Room Status.

Check In/Check Out Status

The attendant can review the check-in/check-out status by assigning an **occ-rooms** (occupied rooms) button on the Attendant Console screen.

When the attendant activates check-in/check-out mode, the DXS lamps light for every occupied room.

Maid Status

The attendant can review the maid status by assigning a **maid-stat** button on the Attendant Console screen.

When the attendant activates the maid status mode, the system prompts the attendant to enter the room status number (1 to 6) that they want to review. You can define these six room states on the Hospitality screen. Once they enter a room state, the display shows the definition of the room state and lights the DXS lamps for every room in that state.

While the console is in maid status mode, the attendant can review another room state by entering the room status number.

Note:

The attendant cannot make outgoing calls through the keypad while the console is in maid status mode; they must return to normal mode.

Chapter 33: Attendant Serial Calling

Using the Attendant Serial Calling feature, the attendant can transfer trunk calls that the system routes to the attendant when the user disconnects the call. The attendant can then transfer the call to another user who is on the same server.

Detailed description of Attendant Serial Calling

You can administer the system to route calls to the attendant when the called user hangs up, but the caller does not. The attendant can then use Attendant Serial Calling to transfer the call to another user, at the request of the caller. The attendant can transfer calls only to those users on the same server.

This feature helps the attendant to use the trunks efficiently. If few trunks are available, and direct inward dialing (DID) is unavailable, a caller might make several attempts to complete a call before the caller is successful. When a caller makes a successful call to the attendant, the user can use the same line into the server for multiple telephone calls.

The attendant display shows the attendant that an incoming call is a serial call.

Attendant Serial Calling administration

This section describes the prerequisites and the screens for the Attendant Serial Calling feature.

Preparing to administer Attendant Serial Calling

Procedure

Set up an attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Serial Calling

Screen name	Purpose	Fields
Attendant Console	Administer the serial-cal button	Any available button field in the **Feature Button Assignments** area

Chapter 34: Attendant Split Swap

Using the Attendant Split Swap feature, an attendant can alternate between an active call and a split call. This feature is useful when the attendant must transfer a call, but first must talk independently with each party before completing the transfer.

Detailed description of Attendant Split Swap

With the Attendant Split Swap feature, an attendant can alternate between an active call and a split call. To activate this feature, the attendant presses a button on the attendant console.

Attendant Split Swap administration

The following task is part of the administration process for the Attendant Split Swap feature:

- Assigning a split-swap button

Related links

Assigning a split-swap button on page 237

Preparing to administer Attendant Split Swap

Procedure

Set up the attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Split Swap

Screen name	Purpose	Fields
Attendant Console	Assign a split-swap button.	Any unassigned button in the **Feature Button Assignments** area.

Assigning a split-swap button

Procedure

1. Type `change attendant n`, where *n* is the number of the attendant console. Press `Enter`.
2. On the Attendant Console screen, click `Next` until you see the **Feature Button Assignments** area.
3. In the **Feature Button Assignments** area, assign `split-swap` to an available button.
4. Press `Enter` to save your changes.

Chapter 35: Attendant Timers

The Attendant Timers feature automatically alert the attendant after an administered time interval for which the calls remain waiting or on hold. The attendant can then reconnect with the caller and decide whether to terminate the call or continue waiting.

Detailed description of Attendant Timers

Attendant Timers automatically alert the attendant after an administered time interval for the following types of calls:

- Extended calls that are waiting to be answered or waiting to be connected to a busy single-line telephone
- One-party calls that are on hold at the console
- Transferred calls that are unanswered after a transfer

The Attendant Timers feature informs the attendant that a call requires additional attention. After the attendant reconnects to the call, the user can either choose to try another extension number, disconnect, or continue to wait.

Communication Manager supports a variety of administrable attendant timers. Attendant timers include:

- Unanswered DID Call Timer. Specifies how long a direct inward dialing (DID) call can go unanswered before the system routes the call to the administered DID, TIE, or ISDN intercept treatment.
- Attendant Return Call Timer. Unanswered calls that the attendant extends return to the same attendant, if the attendant is available. If the same attendant is unavailable, unanswered calls return to the attendant group queue.

  The Attendant Return Call Timer is not set for calls that are extended from one attendant to another attendant. The system redirects a transferred call that times out to an attendant after the interval that is administered for the Attendant Return Call timer.
- Attendant Timed Reminder of Held Call Timer. Specifies how long a call is held. When the timer expires, the held call alerts the attendant. The attendant's screen displays the message `hc`. You can administer either a high-pitched ring or a primary alert.
- Attendant No-Answer Timer. Specifies how long a call that terminates at an attendant console can ring with primary alerting. When the timer expires, the call rings with a secondary,

higher-pitch ring. The ringing pattern of a disabled Attendant No Answer Timer remains the same for the primary pattern and the secondary pattern. If the call remains unanswered during this interval, the system routes the call to the attendant group and console where the call was placed in a Position Busy state. This timer does not apply to calls that are placed to the extension of the attendant, or to calls that the attendant originates.

- Attendant Alerting Interval (Timed Reminder). Specifies how long a call that terminates at an attendant console can ring with secondary alerting. When the timer expires, the attendant console is placed into position busy mode, and the system forwards the call to the attendant group. If the console where the alerting interval is reached is the last active day console, the system goes into Night Service, if Night Service is enabled. This timer does not apply to calls that are placed to the extension of the attendant, or to calls that the attendant originates.

  You can disable the alerting interval. In this case, a call continues to ring at the extension of the original attendant until the caller hangs up, or another feature disconnects the call. If the call reaches the timeout limit for unanswered DID calls during Night Service, for example, the Night Service feature disconnects the call.
- Line Intercept Tone Timer. Specifies how long line intercept can be. For example, LITT:10 seconds means that line intercept stops after 10 seconds.

Attendant Timers administration

The following task is part of the administration process for the Attendant Timers feature:

- Setting up Attendant Timers

Related links

Setting up Attendant Timers on page 240

Preparing to administer Attendant Timers

Procedure

Set up the attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Timers

Screen name	Purpose	Fields
Console Parameters	Set up the timers for the attendant.	All fields in both the **Timing** and the **Incoming Call Reminders** areas

Setting up Attendant Timers

Procedure

1. Type `change console-parameters`. Press `Enter`.
2. On the Console Parameters screen, click `Next` until you see the **Timing** area.
3. In the **Timing** area, complete the following fields:
   - In the **Time Reminder on Hold (sec)** field, type the number of seconds before a split call returns to the console. Valid entries are a number from 10 to 1024, or blank. A split call can be a call that the attendant extended to a user and is ringing at the user telephone, or otherwise split away from the console.

     Allow 5 seconds for each ring at all points in a coverage path to ensure that the entire path is completed before the call returns to the console.
   - In the **Return Call Timeout (sec)** field, type the number of seconds that a call remains on hold at the console before the system alerts the attendant. In a Centralized Attendant Service (CAS) arrangement, administer the main console and the branch consoles with the same value. Valid entries are a number from 10 to 1024, or blank.
   - In the **Time in Queue Warning (sec)** field, type the number of seconds that a call can remain in the attendant queue before the system alerts the attendant. Valid entries are a number from 9 to 999.
4. In the **Incoming Call Reminders** area, complete the following fields:
   - In the **No Answer Timeout (sec)** field, type the number of seconds that a call to the attendant can remain unanswered without invoking a more insistent-sounding tone. Valid entries are a number from 10 to 1024, or blank.

     Allow 5 seconds for each ring at all points in a coverage path to ensure that the entire path is completed before the call returns to the console.
   - In the **Alerting (sec)** field, type the number of seconds after which the system disconnects a held call or an unanswered call from an attendant loop. The system routes the disconnected call either to another attendant or to Night Service. Valid entries are a number from 10 to 1024, or blank.
   - In the **Secondary Alert on Held Reminder Calls?** field, perform one of the following actions:
     - If you want to start attendant alerting for Held Reminder Calls with secondary alerting, type `y`
     - If you want to have Held Reminder Calls alert the attendant in the same way as normal calls, type `n`. Normal calls start with primary alerting, and then change to secondary alerting when the No Answer Timeout expires.
5. Press `Enter` to save your changes.

Interactions for Attendant Timers

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

Call Coverage

If a telephone user transfers a call to an on-premises telephone, and the call remains unanswered at the expiration of the Timed Reminder Interval, the system redirects the call to an attendant. Redirection occurs even if the call redirects through Call Coverage or Call Forwarding from the transferred-to telephone.

The system redirects an attendant-extended call to coverage instead of returning the call to an attendant if the coverage criteria is met before the Timed Reminder Interval expires. However, the system returns unanswered calls to an attendant at the expiration of the interval.

For any call that alerts an attendant as a coverage call, that is, for any unanswered station-to-station call with the “attd” (attendant) in the Coverage Path screen of the called telephone, the secondary alerting tone goes mute.

Centralized Attendant Service

If an attendant at the main location transfers a call from a branch location to an extension at the main location, the timed reminder does not apply, and the call does not return to the attendant if the call is unanswered.

Return Call to (same) Attendant

Communication Manager provides improvements to the existing attendant features with Return Call to (same) Attendant feature from release 5.2 onwards.

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

Communication Manager provides individual queuing functions for each attendant supporting a multiplicity of waiting calls at a given time from release 5.2 onwards. When at least one call is waiting in the above queue, the Individual Calls Waiting Indicator is displayed in red. Calls queue as long as the attendant is busy.

When the feature Return Call to (same) Attendant is enabled, a call returning to a busy or now unavailable same attendant is placed into an individual waiting queue for this attendant, instead of queuing it into the attendant group. A waiting Return Call moves from the attendant’s queue to the attendant group’s queue after a certain period of time.

The field **Overflow timer to Group Queue** is extended to page 2 of the console-parameters screen.

Attendant Overflow Timer

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

Chapter 36: Attendant Trunk Identification

An attendant or a user can use the Attendant Trunk Identification feature to identify a faulty trunk.

Detailed description of Attendant Trunk Identification

With Attendant Trunk Identification, the attendant, or a user with a display, can identify a faulty trunk. When the attendant or user presses the trk-id button, the system displays the Trunk Access Code (TAC) and trunk member number of a call. The trunk can then be removed from service.

Attendant Trunk Identification administration

This section describes the prerequisites and the screens for the Attendant Trunk Identification feature.

Preparing to administer Attendant Trunk Identification

Procedure

Set up an attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Attendant Trunk Identification

Screen name	Purpose	Fields
Attendant Console	Administer the trk-id button for the Attendant Trunk Identification feature	Any available button field in the **Feature Button Assignments** area
Station	Administer the trk-id button for the Attendant Trunk Identification feature	Any available button field in the **Feature Button Assignments** area

Chapter 37: Attendant Vectoring

Use the Attendant Vectoring feature to provide attendants with a flexible way to manage incoming calls. For example, without Attendant Vectoring, calls that the system redirects from the attendant console to a night telephone can ring only at that telephone. These calls do not follow a coverage path. With Attendant Vectoring, Night Service calls follow the coverage path of the night telephone. The coverage path can go to another telephone, and eventually to a voice mail system. The caller can then leave a message that can be retrieved at any time.

Detailed description of Attendant Vectoring

With the Attendant Vectoring feature, you can establish an attendant vector directory number (VDN), and send attendant group calls through vector processing. This feature is useful when you want flexibility with how the system routes calls when the system is in Night Service mode.

Attendant Vectoring takes precedence over all local attendant codes that you administer. If Attendant Vectoring is enabled, the system uses call vectors instead of the normal attendant call routing to process attendant-seeking, or dial 0, calls.

For more information about vectors and VDNs, see the Meet-Me Conference feature. See also the *Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*.

Attendant Vectoring administration

The following tasks are part of the administration process for the Attendant Vectoring feature:

- Creating a VDN extension for Attendant Vectoring
- Assigning the VDN extension for Attendant Vectoring to a console
- Assigning the VDN extension for Attendant Vectoring to a tenant

Related links

Creating a VDN extension for Attendant Vectoring on page 246
Assigning the VDN extension for Attendant Vectoring to a console on page 247
Assigning the VDN extension for Attendant Vectoring to a tenant on page 247

Preparing to administer Attendant Vectoring

Procedure

1. Set up the attendant console.

   For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

2. On the Optional Features screen, verify that the **Attendant Vectoring** field is set to y.

   a. To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

   b. Click `Next` until you see the **Attendant Vectoring** field. Ensure that the **Attendant Vectoring** field is set to y.

   Note:

   You cannot use Attendant Vectoring with the Centralized Attendant Service (CAS) feature. Therefore, the **Attendant Vectoring** field cannot be set to y if either the **CAS Branch** field or the **CAS Main** field on the Optional Features screen is set to y.

   Your license file sets the values in these fields. You cannot manually change these values. If you have any questions related to Communication Manager licensing, go to the Avaya Support website at http://support.avaya.com and download the related documentation and knowledge articles.

3. On the Call Vector screen, verify that the **Attendant Vectoring** field is set to y.

   a. To view the Call Vector screen, type `change vector n`, where *n* is the number of a vector. Press `Enter`.

   b. The Call Vector screen, displays the **Attendant Vectoring** field only if on the Optional Features screen, you set the **Attendant Vectoring** field to y.

   Note:

   You cannot use the same vector for both Attendant Vectoring and the Meet-me Conference features. Therefore, the **Attendant Vectoring** field and the **Meet-me Conference** field cannot both be set to y at the same time.

Screens for administering Attendant Vectoring

Screen name	Purpose	Fields
Optional Features	Activate the Attendant Vectoring feature	Attendant Vectoring

Table continues…

Screen name	Purpose	Fields
	• Verify the Attendant Vectoring feature on the Call Vector screen • Administer the Attendant Vectoring feature on the Console Parameters screen See the “Prerequisites” section for the correct settings	Tenant Partitioning
Call Vector	Set the Attendant Vectoring field to y	Attendant Vectoring
Vector Directory Number	Create an Attendant Vectoring VDN extension	Attendant Vectoring
Console Parameters	Assign the Attendant Vectoring VDN extension to a console	Attendant Vectoring VDN
Tenant	Assign the Attendant Vectoring VDN extension to a tenant	Attendant Vectoring VDN

Creating a VDN extension for Attendant Vectoring

About this task

Use the Vector Directory Number screen to define vector directory numbers (VDNs) for the Call Vectoring feature. A VDN is an extension that gives you access to a call vector. Each VDN is mapped to one call vector.

VDNs are not assigned to physical equipment. You gain access to a VDN through direct dial central office (CO) trunks that are mapped to the VDN, direct inward dial (DID) trunks, and listed directory number (LDN) calls. The VDN can be a night destination for LDN.

Procedure

1. Type `change vdn n`, where *n* is the VDN extension. Press `Enter`.

   The system displays the Vector Directory Number screen.

2. In the **Attendant Vectoring** field, perform one of the following actions:
   - If you want this VDN to be an attendant vector, type `y`.
   - If you do not want this VDN to be an attendant vector, type `n`.

     You cannot use Attendant Vectoring with the Meet-me Conference feature. Therefore, the **Attendant Vectoring** field and the **Meet-Me Conferencing** field cannot both be set to `y` at the same time.

3. Press `Enter` to save your changes.

Assigning the VDN extension for Attendant Vectoring to a console

Before you begin

The Console Parameters screen displays the **Attendant Vectoring VDN** field only if, on the Optional Features screen:

- **Attendant Vectoring** field is set to `y`
- **Tenant Partitioning** field is set to `n`

Procedure

1. Type `change console-parameters n`, where *n* is the assigned number of the attendant console. Press `Enter`.

   The system displays the Console Parameters screen.

2. In the **Attendant Vectoring VDN** field, type the VDN extension that you have created for Attendant Vectoring.
3. Press `Enter` to save your changes.

Assigning the VDN extension for Attendant Vectoring to a tenant

About this task

Use the Tenant screen to define tenants that access the system. If your server uses more than one tenant, see the Tenant Partitioning feature for more information.

Procedure

1. Type `change tenant n`, where *n* is the assigned number of the tenant. Press `Enter`.

   The system displays the Tenant screen.

2. In the **Attendant Vectoring VDN** field, type the VDN extension that you created for Attendant Vectoring.
3. Press `Enter` to save your changes.

Related links

Tenant Partitioning on page 1341

Considerations for Attendant Vectoring

This section provides information about how the Attendant Vectoring feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Vectoring under all conditions. The following considerations apply to Attendant Vectoring:

- Teletypewriter device (TTY) for the hearing impaired

Unlike fax machines and modems, a TTY has no handshake tone and no carrier tone. A TTY is silent when not transmitting. Systems cannot automatically identify TTY callers.

However, the absence of these special tones also means that voice and TTY tones can be intermixed in prerecorded announcements. The ability to provide a hybrid voice-and-TTY announcement, when combined with the Attendant Vectoring capability, can permit a single telephone number to accommodate both voice and TTY callers.

Interactions for Attendant Vectoring

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

Centralized Attendant Service (CAS)

You cannot use Attendant Vectoring with the Centralized Attendant Service (CAS) feature. Therefore, the **Attendant Vectoring** field cannot be set to y if either the **CAS Branch** field or the **CAS Main** field on the Optional Features screen is set to y.

Meet-me Conference

You cannot use Attendant Vectoring with the Meet-me Conference feature. Therefore, the **Attendant Vectoring** field and the **Meet-me Conference** field cannot both be set to y at the same time.

Call Coverage and Tenant Partitioning

If a covered call does not route to an attendant in the first tenant group, you can route it to an attendant group of a different tenant partition. For example, you can reroute a call to Tenant Group B if the call is to cover to an attendant for Tenant Partition A but does not route to the attendant or is received out of hours when Attendant Group A is unstaffed.

To reroute the covered calls to another tenant attendant group, Tenant Attendant group B in this example,

1. In the vector for the tenant A attendant vectoring VDN, add a failure branch to a **route-to ldn_number with cov y if unconditionally** step for the LDN extension for the tenant group B TN number.
2. Set the **with coverage** parameter of the route-to step must be set to **cov y** because the calls are covered. Else, the calls don’t route to the VDN. Also, set the **Cvg Enabled for VDN Route-to party?** field of original coverage path, which covers to Tenant A Attendant vectoring VDN, to **y**.

Chapter 38: Audible Message Waiting

Use the Audible Message Waiting feature to alert a user that a message is waiting. The user hears a stutter dial tone when the user goes off hook.

The Audible Message Waiting feature is particularly useful for visually impaired people who cannot see a message waiting light.

Detailed description of Audible Message Waiting

Use the Audible Message Waiting feature to alert a user that a message is waiting. When the user goes off hook, the user hears a stutter tone just before the usual dial tone begins.

Users can access waiting messages from:

- The system memory, where a user can use a display or a voice synthesizer
- A Property Management System (PMS)
- An Avaya Aura® Messaging and Avaya Messaging voice message system

You must ensure that your users know how to retrieve their messages.

You usually assign Audible Message Waiting on telephones without message waiting lights, such as analog telephones.

If the system loses synchronization between telephones and message-status data, use the Clear Message Waiting Indicators to turn off the message waiting indicators.

Audible Message Waiting requires a separate software right-to-use fee.

Audible Message Waiting might be inapplicable in countries that restrict the characteristics of dial tones that the system provides to users.

Audible Message Waiting administration

The following task is part of the administration process for the Audible Message Waiting feature:

- Administering Audible Message Waiting for a user

Related links

Administering Audible Message Waiting for a user on page 250

Preparing to administer Audible Message Waiting

Procedure

View the Optional Features screen, and ensure that the **Audible Message Waiting** field is set to `y`.

If the **Audible Message Waiting** field is set to n, your system is disabled for the Audible Message Waiting feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Audible Message Waiting, or to open a service request.

To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

Screens for administering Audible Message Waiting

Screen name	Purpose	Fields
Optional Features	Enable Audible Message Waiting for your system	Audible Message Waiting
Station	Administer Audible Message Waiting for a user	Audible Message Waiting

Administering Audible Message Waiting for a user

Procedure

1. Type `change station n`, where *n* is the extension of the user for whom you want to activate Audible Message Waiting. Press `Enter`.

   The system displays the Station screen.

2. In the **Audible Message Waiting** field, perform one of the following actions:

   - If you want the user to hear the stutter dial tone if a message is waiting when the user goes off hook, type `y`.
   - If you do not want the user to the hear stutter dial tone if a message is waiting when the user goes off hook, type `n`.

   The system displays the **Audible Message Waiting** field only if the **Audible Message Waiting** field on the Optional Features screen is set to `y`.

   Note:

   Note that the **Audible Message Waiting** field does not control the Message Waiting lamp.

Considerations for Audible Message Waiting

This section provides information about how the Audible Message Waiting feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Audible Message Waiting under all conditions. The following considerations apply to Audible Message Waiting:

- You must tell the user where to call to retrieve messages if the messages are not stored in the system memory for users to access by way of a display or a voice synthesizer.

Interactions for Audible Message Waiting

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

China Special Dial Tone

The Audible Message Waiting feature interacts with the Special Dial Tone feature. This interaction is for customers in China only. This feature plays a special dial tone whenever an analog telephone would normally receive dial tone, but the user needs to know about a feature or condition that is active at the telephone. Examples of such features or conditions include features that can be activated and deactivated by using a FAC from the telephone, and cause some rerouting of calls to that telephone.

Chapter 39: AUDIX One-Step Recording

Use the AUDIX One-Step Recording feature to record telephone conversations by pressing a single button. The AUDIX One-Step Recording feature uses Avaya Aura® Messaging and Avaya Messaging to record a telephone conversation. A user needs to press only one feature button on the telephone to activate this feature. AUDIX One-Step Recording then stores the recorded conversation as a message in the voice mailbox of the user. The system activates AUDIX One-Step Recording only after a call is answered.

The AUDIX One-Step Recording feature is also known as Record on Messaging.

Note:

Some countries, states, and localities have laws that determine if and under what circumstances you can record telephone conversations. Before you administer the AUDIX One-Step Recording feature, you must understand and comply with these laws.

Detailed description of AUDIX One-Step Recording

The AUDIX One-Step Recording feature is available with Communication Manager Release 1.3 (V11) or later.

- Communication Manager Release 7.1.3 and later supports Avaya Aura® Messaging and Avaya Messaging.
- Communication Manager Release 2.0 and later supports AUDIX One-Step Recording with local Avaya Aura® Messaging and Avaya Messaging system or with remote Avaya Aura® Messaging and Avaya Messaging system. To use remote Avaya Aura® Messaging and Avaya Messaging system, the person recording the conversation must have Communication Manager Release 2.0 or later.

AUDIX One-Step Recording feature button

The AUDIX One-Step Recording feature uses an administered feature button, **audix-rec**. The administrator uses the Station screen to assign this button for each telephone. When you assign the feature button, the system requires you to provide the extension for the Avaya Aura® Messaging and Avaya Messaging hunt group of the user. Users cannot access AUDIX One-Step Recording on any telephone that does not have an administrable feature button, or on an attendant console.

AUDIX One-Step Recording language options

Five languages are available for the feature button labels for AUDIX One-Step Recording:

- English
- Italian
- French
- Spanish
- A user-defined language

The feature button labels for AUDIX One-Step Recording are available in English, with predefined Italian, French, and Spanish translations. The administrator cannot change the text of the English, the Italian, the French, or the Spanish feature button labels.

The administrator can translate the feature button labels into a user-defined language. This translation can be any other language that the customer chooses, such as German. The administrator can use only one user-defined language throughout the system.

AUDIX One-Step Recording periodic alerting tone

While Avaya Aura® Messaging and Avaya Messaging record the conversation, all parties on the call might hear a periodic alerting tone. This alerting tone reminds all parties on the call that Avaya Aura® Messaging and Avaya Messaging are recording the conversation. The tone that plays is a zip tone.

You choose the time interval to play the periodic alerting tone. If you set the time interval of the periodic alerting tone to zero, the parties hear no alerting tone.

AUDIX One-Step Recording ready indication tone

When Avaya Aura® Messaging and Avaya Messaging start recording a conversation, the system plays a ready indication tone. The tone that is played is a zip tone.

You can administer the **Apply Ready Indication Tone To Which Parties In The Call** field to play the ready indication tone to:

- All the parties on the call.

  The initiator only. The initiator is the user who activates the AUDIX One-Step Recording feature.

- None of the parties on the call.

Note:

When the **Apply Ready Indication Tone To Which Parties In The Call** field is set to `initiator`, and the Audix record button is pressed on H323 phone, then the ready indication tone is heard on initiator H323 endpoint only. For other phone types, all parties in the call can hear the indication tone. When the **Apply Ready Indication Tone To Which Parties In The**

Call field is set to `all` and the **Interval For Applying Periodic Alerting Tone (seconds)** field is set to `0`, the parties in the call do not hear the ready indication tone and the alerting tone.

AUDIX One-Step Recording delay timer

When the user presses the **audix-rec** feature button, Avaya Aura® Messaging and Avaya Messaging answer. After Avaya Aura® Messaging and Avaya Messaging answer, the system uses the recording delay timer to wait for Avaya Aura® Messaging and Avaya Messaging to get ready to interpret digits. The system then sends digit 1 to tell Avaya Aura® Messaging and Avaya Messaging to start recording.

The recording delay timer is preset to 500 milliseconds. This delay is sufficient for most recorded conversations. If you have to change this setting, see the section titled Assigning AUDIX One-Step Recording Parameters.

AUDIX One-Step Recording zip tone_release #_

When the AUDIX One-Step Recording feature is recording a conversation, the tone that a user hears is a zip tone. By default, a zip tone plays at a frequency of 480 Hz for 500 milliseconds, followed by silence.

If you need to change the characteristics of the zip tone, the screen that you use depends on what version of Communication Manager you have.

AUDIX One-Step Recording administration

The following tasks are part of the administration process for the AUDIX One-Step Recording feature:

- Assigning AUDIX One-Step Recording Parameters
- Translating AUDIX One-Step Recording telephone feature buttons and labels
- Assigning the AUDIX One-Step Recording feature button
- Changing the zip tone for AUDIX One-Step recording for release 1.3 (V11) or earlier
- Changing the zip tone for AUDIX One-Step Recording for release 2.0 (V12) or later

Related links

Assigning AUDIX One-Step Recording Parameters on page 255
Translating AUDIX One-Step Recording telephone feature buttons and labels on page 256
Assigning the AUDIX One-Step Recording feature button on page 257
Changing the zip tone for AUDIX One-Step recording for release 1.3 (V11) or earlier on page 258
Changing the zip tone for AUDIX One-Step Recording for release 2.0 (V12) or later on page 258

Preparing to administer AUDIX One-Step Recording

Procedure

On the Optional Features screen, ensure that the **G3 Version** field is set to `V11` or later.

If this field is not set to `V11` or later, your system is disabled for the AUDIX One-Step Recording feature. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to AUDIX One-Step recording, or to open a service request.

To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

Screens for administering AUDIX One-Step Recording

Screen name	Purpose	Fields
Optional Features	Ensure that you have Communication Manager version 1.3 (V11) or later	G3 Version
Feature-Related System Parameters	Set the time interval, in milliseconds, for the recording delay timer	Recording Delay Timer (msec)
	Assign who on the call can hear the ready indication tone	Apply Ready Indication Tone To Which Parties In The Call
	Set the time interval, in seconds, for the periodic alerting tone	Interval For Applying Periodic alerting tone (seconds)
Language Translations	If needed, change the translation of the **audix-rec** feature button to a user-defined language	Audix Recording
	If needed, change the translation of the **Audix Record** button label to a user-defined language	Audix Record
Station	Assign the **audix-rec** feature button and associate the hunt group extension of the user	Button Assignments

Assigning AUDIX One-Step Recording Parameters

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. On the Feature-Related System Parameters screen, click `Next` until you see the **AUDIX One-step Recording** section.
3. If you need to change the time between when Avaya Aura® Messaging and Avaya Messaging answers and when Avaya Aura® Messaging and Avaya Messaging start recording, change the value in the **Recording Delay Timer (msec)** field.

   After Avaya Aura® Messaging and Avaya Messaging start recording, Communication Manager must filter out the Avaya Aura® Messaging and Avaya Messaging tone. The

user must wait longer than the Recording Delay Timer setting before the user notices that recording has started.

4. In the **Apply Ready Indication Tone To Which Parties In The Call** field, type one of the following values.
   - If you want all parties on the call to hear the ready indication tone, leave the default set to `all`. The screen displays the **Interval For Applying Periodic Alerting Tone (seconds)** field.
   - If you want only the initiator to hear the ready indication tone, right-click the field and select `initiator`. The screen does not display the **Interval For Applying Periodic Alerting Tone (seconds)** field.
   - If you want no one on the call to hear the ready indication tone, right-click the field and select `none`. The screen does not display the **Interval For Applying Periodic Alerting Tone (seconds)** field.
5. In the **Interval For Applying Periodic Alerting Tone (seconds)** field, type a value between 0 and 60 seconds.
6. Press `Enter` to save your changes.

Translating AUDIX One-Step Recording telephone feature buttons and labels

Procedure

1. Translate the AUDIX One-Step Recording text that appears on a telephone display to a user-defined language.
2. Translate the AUDIX One-Step Recording button label to a user-defined language.

Translating the AUDIX One-Step Recording text that appears on a telephone display to a user-defined language

Procedure

1. Type `change display-messages view-buttons`. Press `Enter`.
2. On the Language Translations screen, click `Next` until you see the **Audix Recording** field.
3. In the **Translation** field, type a translated name for Audix Recording into the user-defined language.

   Note:

   The language translations for the English, the Italian, the French, and the Spanish feature display are predefined. You cannot change the text for these translations.
4. Press `Enter` to save your changes.

Translating the AUDIX One-Step Recording button label to a user-defined language

About this task

The 2420 DCP telephone and the 4620 IP telephone have digital button labels instead of paper labels. If you need to translate the AUDIX One-Step Recording button labels into a user-defined language for these telephones, follow this procedure.

Procedure

1. Type `change display-messages button-labels`. Press `Enter`.
2. On the Language Translations screen, click `Next` until you see the **Audix Record** field.
3. In the **Translation** field, type a translated name for the Audix Record button label into the user-defined language.

   Note:

   The language translations for the English, the Italian, the French, and the Spanish feature buttons are predefined. You cannot change the text for these translations.
4. Press `Enter` to save your changes.

Assigning the AUDIX One-Step Recording feature button

Procedure

1. Type `change station` *n*, where *n* is the extension of the telephone. Press `Enter`.
2. On the Station screen, click `Next` until you see the **Button Assignments** area.
3. Right-click a button field that is not assigned to see a list of button names.
4. Select `audix-rec` from the list.
5. In the **Ext** field, type the Avaya Aura® Messaging and Avaya Messaging hunt group extension of the user.
6. Press `Enter` to save your changes.

Change the zip tone for AUDIX One-Step recording

When the AUDIX One-Step Recording feature is recording a conversation, the tone that a user hears is a zip tone. By default, a zip tone plays at a frequency of 480 Hz for 500 milliseconds, followed by silence.

If you need to change the characteristics of the zip tone, the screen that you use depends on what version of Communication Manager you have.

Changing the zip tone for AUDIX One-Step recording for release 1.3 (V11) or earlier

Procedure

1. Enter `change system-parameters country-options`.
2. On the System Parameters Country-Options screen, click `Next` until you see either:
   - An existing System Parameters Country-Options screen for the zip tone.

     If a screen already exists for the zip tone, the word “zip” appears in the **Tone Name** field.
   - A blank System Parameters Country-Options screen.

     If a screen already exists for the zip tone, skip the next step and go to Step 4.
3. Right-click the **Tone Name** field to see a list of options. Select zip from the list.
4. Right-click the **Cadence Step 1** field to see a list of options. Select a tone frequency and level combination from the list.
5. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to play.
6. Right-click the **Cadence Step 2** field to see a list of options. Select `silence` from the list.
7. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to remain silent after the system plays the tone.
8. Select **Enter** to save your changes.

Changing the zip tone for AUDIX One-Step Recording for release 2.0 (V12) or later

Procedure

1. Enter `change tone-generation`.
2. On the Tone Generation screen, click `Next` until you see either:
   - An existing Tone Generation Customized Tones screen for the zip tone

     If a screen already exists for the zip tone, the word “zip” appears in the **Tone Name** field.
   - A blank Tone Generation Customized Tones screen.

     If a screen already exists for the zip tone, skip the next step and go to Step 4.
3. Right-click the **Tone Name** field to see a list of options.
4. Select `zip` from the list.
5. Right-click the **Cadence Step 1** field to see a list of options.
6. Select a tone frequency and level combination from the list.

   The screen displays a **Duration (msec)** field.

7. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to play.
8. Right-click the **Cadence Step 2** field to see a list of options.
9. Select `silence` from the list.

   The screen displays a **Duration (msec)** field.
10. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to remain silent after the system plays the tone.
11. Select **Enter** to save your changes.

End-user procedures for AUDIX One-Step Recording

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Recording a conversation with AUDIX One-Step Recording

About this task

The user who wants to record the conversation is called the “initiator.”

Note:

This procedure assumes that the initiator understands and complies with any country, state, and local laws concerning if you can record telephone conversations.

Procedure

1. A user announces to the other parties on the call that he or she wants to record the conversation.
2. This user gets permission from the parties, and presses the **audix-rec** button to record the conversation.

   When the initiator presses the `audix-rec` button, the LED for the audix-rec button flashes. After a few seconds, the telephone displays of all internal users on the call change to Conference. The number of parties on the call increases by one. The LED on the telephone of the initiator stays on, and no longer flashes. This light indicates that Avaya Aura® Messaging and Avaya Messaging are ready to record.

   Avaya Aura® Messaging and Avaya Messaging start to record the conversation. The system plays the ready indication tone to indicate that recording is started. Only the initiator hears any Avaya Aura® Messaging and Avaya Messaging announcements.
3. To stop the recording at any time, the initiator can press the `audix-rec` button again.

   The LED on the telephone of the initiator goes out. The number of parties on the call decreases by one. The call remains active. The initiator can press the `audix-rec` button

to start and stop recording the same conversation any number of times. Each time creates a separate recorded message.

If the initiator hangs up while Avaya Aura® Messaging and Avaya Messaging are recording the conversation, the recording ends. If the call is originally a two-party call and the other party hangs up, the recording ends. If the call is originally a multiple-party conference call and someone other than the initiator hangs up, the recording continues.

When the recording ends, the system saves the recorded conversation in the voice mailbox of the initiator as a new voice mail message.

Considerations for AUDIX One-Step Recording

This section provides information about how the AUDIX One-Step Recording feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of AUDIX One-Step Recording under all conditions. The following considerations apply to the AUDIX One-Step Recording feature:

Capacity constraints and feature limitations

AUDIX One-Step Recording has the following capacity constraints and feature limitations:

- Only one simultaneous Avaya Aura® Messaging and Avaya Messaging recording is allowed for each call.
- The **audix-rec** feature button works as a toggle button. When the button is active, the button is associated with only one call. A user cannot use the **audix-rec** feature button on two calls simultaneously.
- Attendant consoles do not have an **audix-rec** feature button. Attendants cannot use the AUDIX One-Step Recording feature.
- Service observers who are actively involved in service observing cannot use the AUDIX One-Step Recording feature.

Denial scenarios

The AUDIX One-Step Recording feature is denied, and the feature button flutters, if a user presses the **audix-rec** button when:

- No call is active on the telephone
- The user is still dialing digits
- The connection to Avaya Aura® Messaging and Avaya Messaging are not operating
- All Avaya Aura® Messaging and Avaya Messaging ports are busy
- The number of parties on the call reaches the administered maximum
- Another party on the call is already recording the conversation with AUDIX One-Step Recording
- The user starts the recording from a bridged call appearance

- Service observers are actively involved in service observing
- The incoming or outgoing call is ringing and is not answered

Security

Some countries, states, and localities have laws that determine if and under what circumstances you can record telephone conversations. Before you administer the AUDIX One-Step Recording feature, you must understand and comply with these laws.

Serviceability

This feature depends on Avaya Aura® Messaging and Avaya Messaging to function. The administrator is responsible for properly administering Avaya Aura® Messaging and Avaya Messaging. Avaya Aura® Messaging and Avaya Messaging must work for the telephone user before the administrator applies this feature to the telephone. Specifically, the administrator needs to set the appropriate Mailbox Size and Voice Mail Message Maximum Length on Avaya Aura® Messaging and Avaya Messaging for the user.

The **audix-rec** button requires the extension of the Avaya Aura® Messaging and Avaya Messaging hunt group of the user. The administrator must type the correct extension on the Station screen.

Interactions for AUDIX One-Step Recording

This section provides information about how the AUDIX One-Step Recording feature interacts with other features in your system. Use this information to ensure that you receive the maximum benefits of AUDIX One-Step Recording in any feature configuration. The following interactions apply to the AUDIX One-Step Recording feature:

Bridged Call Appearance

- A user cannot activate or deactivate the **audix-rec** feature button from a bridged call appearance.
- If the administrator sets the ready indication tone to play to all parties, parties on bridged call appearances hear the tone. If the administrator sets the ready indication tone to play to the initiator only, parties on bridged call appearances do not hear the tone.

Call Park

When AUDIX One-Step Recording is active on a call, you cannot park the call. If the user attempts to park the call, the call appearance LED flutters.

When a call is parked, you cannot activate the AUDIX One-Step Recording feature. If the user attempts to activate AUDIX One-Step Recording, the feature button LED flutters.

Conference

When the recording request is in process, the LED is flashing. If anyone attempts to conference in another party, AUDIX One-Step Recording stops. The LED goes out.

When the recording starts, the LED is on but not flashing. Any party on the call can conference in another party. The recording continues.

If AUDIX One-Step Recording is in progress on two separate calls, you cannot conference the two calls together.

Coverage Answer Group

An answer group contains up to 100 members who act as a coverage point for another user. For example, if several attendants are responsible to answer redirected calls from a department, assign all attendants to an answer group. The administrator assigns a group number to the answer group. The system displays the group number in the coverage path of that department. All telephones in an answer group ring simultaneously. Any member of the group can answer the call.

When a member of a Coverage Answer Group answers a call, any of the parties on the call can press the **audix-rec** button to record the conversation. The system stores the recorded message in the voice mailbox of the party who answers the call.

Drop Last

After Avaya Aura® Messaging and Avaya Messaging start to record, the initiator becomes the control party. If the initiator presses the **Drop** button, AUDIX One-Step Recording stops and the LED goes out. If other parties on the call press the **Drop** button, the system denies the request.

As a conference initiator, you can add other users to a call using the conference operation. If a pickup group member picks up the call and when the conference initiator presses **drop-last** button, the entire conference is dropped. If the principal user is involved in the call, only the principal is dropped.

Group Paging that uses a speakerphone

With Group Paging, users can make an announcement over a group of digital speakerphones. Neither the group members who receive a page, nor the originator of the page, can use AUDIX One-Step Recording to record the conversation. If anyone on the call presses the **audix-rec** button, the system ignores the request. The LED flutters.

Hunt Group

If a member of a hunt group answers a call, the parties on the call can use AUDIX One-Step Recording to record the conversation. The system stores the recorded message in the voice mailbox of the party who answers the call.

Hunt Group queueing

Users cannot activate AUDIX One-Step Recording when the following conditions apply.

- The queue is enabled for the Avaya Aura® Messaging and Avaya Messaging hunt group
- All the Avaya Aura® Messaging and Avaya Messaging ports are busy

Meet-me Conference

Parties on a Meet-me Conference can use AUDIX One-Step Recording. Conference parties can selectively use the Display and Drop feature to drop the AUDIX One-Step Recording hunt group extension from the call. The LED goes out.

Mode Code interface

Voice mail connections through the Mode Code interface rely on digits that are sent over analog ports. The AUDIX One-Step Recording feature does not work with a Mode Code connection.

Terminating Extension Group (TEG)

Neither group members who receive TEG calls, nor the originators of TEG calls, can use AUDIX One-Step Recording to record the conversation. If anyone on the call presses the **audix-rec** button, the system denies the request. The LED flutters.

Transfer

When the recording request is in process, the LED is flashing. If anyone attempts to transfer the call to another party, AUDIX One-Step Recording stops. The LED goes out.

When the recording starts, the LED is on but not flashing. Any party on the call can transfer the call to another party.

- If the initiator transfers the call, recording automatically stops after the transfer.
- If another party on the call transfers the call, recording continues.

  If AUDIX One-Step Recording is in progress on two separate calls, you cannot transfer one call to the other.

Vector Directory Number (VDN)

When a call is answered through a VDN, any of the parties on the call can press the **audix-rec** button to record the conversation.

Whisper Page

With Whisper Page, no parties on the call can use AUDIX One-Step Recording to record the conversation. If anyone on the call presses the **audix-rec** button, the system denies the request. The LED flutters.

AUDIX One-Step Recording troubleshooting

This section lists the known or common problems that users might experience with the AUDIX One-Step Recording feature.

Problem	Possible cause	Action
The user does not have the **audix-rec** button on the telephone.	The **audix-rec** button is not assigned to the telephone of the user.	Use the **`change station`** *n* command, where *n* is the extension of the telephone, to add the **audix-rec** button.
	The telephone of the user does not support buttons that can be administered.	This user cannot access the AUDIX One-Step Recording feature.
The user hears a beep every few seconds during recording.	The alerting tone interval is set too low.	Set the alerting tone interval to a number that is between 15 and 60.
Nothing happens when the user presses the **audix-rec** button. The button light flutters.	The user was not on an active call.	Inform the user that the **audix-rec** button only works if the user is on an active call.
	The connection to Avaya Aura® Messaging and Avaya Messaging are not operating.	Ensure that Avaya Aura® Messaging and Avaya Messaging are operating correctly. Else, the user must wait for the system to reestablish the connection.

Table continues…

Problem	Possible cause	Action
	The LAN connection between the Avaya Aura® Messaging and Avaya Messaging server and the Communication Manager server is not operating.	Ensure that Avaya Aura® Messaging and Avaya Messaging are operating correctly. Else, the user must wait for the system to reestablish the connection.
	All the Avaya Aura® Messaging and Avaya Messaging ports are busy.	The user must wait for an Avaya Aura® Messaging and Avaya Messaging port to be released.
	Another person on the call is already using the AUDIX One-Step Recording feature to record the conversation.	The user cannot record the conversation if someone else on the call is already using this feature.
	The user attempted to start the AUDIX One-Step Recording feature from a bridged call appearance.	The user cannot record the conversation from a bridged call appearance.
	Remote Avaya Aura® Messaging and Avaya Messaging are configured for Communication Manager Release 1.3.	• Move the voice mail service of the user to a local Avaya Aura® Messaging and Avaya Messaging, or • Upgrade the user to Communication Manager Release 2.0 or later.
The user does not hear a beep during recording.	The ready indication tone is set to play to only the initiator, or to no one.	Set the ready indication tone to all.
	The alerting tone interval is set to zero.	Set the alerting tone interval to a number between 15 and 60.
	The zip tone is set to silence instead of to a frequency and duration.	Reset the characteristics of the zip tone.
After the green LED is steady and the recording starts, the user hears an Avaya Aura® Messaging and Avaya Messaging announcement.	If configured with Avaya Aura® Messaging and Avaya Messaging, ARIA TUI might be turned on. The Recording Delay Timer is not set high enough.	Set the Recording Delay Timer to a higher number.

Chapter 40: Authorization Codes

Use the Authorization Codes feature to control the calling privileges of system users. Authorization codes extend control of calling privileges and enhance security for remote access callers. To maintain system security, Avaya recommends that you use authorization codes.

You can use authorization codes to:

- Override a facilities restriction level (FRL) that is assigned to an originating station or trunk
- Restrict individual incoming tie trunks and remote access trunks from accessing outgoing trunks
- Track Call Detail Recording (CDR) calls for cost allocation
- Provide additional security control

Detailed description of Authorization Codes

When you dial an authorization code, the Facilities Restriction Level (FRL) that is assigned to the extension, the attendant console, the incoming trunk group, or the remote access trunk group that is in use for the call is replaced by the FRL assigned to the authorization code. The FRL that is assigned to the authorization code functions in the same way as the original FRL. However, the new FRL that is assigned to the authorization code might represent greater or lesser calling privileges than the original FRL. Access to any given facility depends on the restrictions associated with the FRL of the authorization code.

The following example shows how authorization codes work with FRLs.

A supervisor is at a desk of an employee. Some employees might have telephone extensions that might not have an FRL assigned to the employees. However, a supervisor can make a call using any telephone if the supervisor has the authorization code assigned to the FRL.

Note:

Ensure the FRL is relevant to the type of call.

Length of authorization codes

For security reasons, authorization codes must consist of 4 to 13 digits. The number of digits in the codes must be a fixed length for a particular server that is running Communication Manager.

Once established, the number of digits (4 to 13) in the authorization code remains fixed unless all codes are removed and reentered. All authorization codes that are used in the system must be the same length.

Using authorization codes

You can administer incoming trunk groups within a system to always require an authorization code. The system applies recall dial tone to a call when the user must dial an authorization code. If the user dials a correct authorization code within 10 seconds (interdigit timeout), the system completes the call as dialed. If the user does not dial an authorization code, or dials an incorrect authorization code, the system routes to the call to an attendant. The system can also route the call to an intercept tone based on how the system was administered.

Usually, Direct Inward Dialing (DID) trunks do not require authorization codes. However, you can administer DID trunks to require an authorization code, but you must do this carefully. Different types of calls can terminate at different endpoints, and requiring an authorization code can be confuse the user.

You can also administer a Cancellation of Authorization Code Request (CACR) digit. The CACR digit cancels the 10-second interval between dialing. When the user dials the CACR digit, the system immediately routes the call according to system administration. Incoming trunk calls receive intercept tone or go to the attendant. Other calls receive intercept tone unless the user's FRL is high enough to route the call. A CACR digit from an off-premises extension over DID and Tie trunks use DID and Tie trunk intercept treatment. Internal calls receive intercept tone.

You must not program passwords or authorization codes onto auto dial buttons. Because display telephones display the programmed buttons, the potential exists for an unauthorized person to use the autodial buttons. If you must program passwords or authorization codes onto auto dial buttons, use the ~s (suppress) character to prevent displaying the codes.

Authorization codes with AAR and ARS calls

Each authorization code is assigned a Class of Restriction (COR) that contains an associated FRL. Within a system, the FRL that is assigned to the point at which the call originates determines the access privileges that are associated with the call. When a user dials an AAR or an ARS call, the system connects or disconnects the call, based on the FRL of the originating station. You use COR to restrict internal or non-AAR or an ARS calls.

You can assign authorization codes to individual users to specify the level of calling privileges. Such codes work regardless of the originating facility. Once an authorization code is required and dialed on an AAR or an ARS call, the FRL assigned to the authorization code replaces the originating FRL. This new FRL controls and defines the privileges of the user.

An AAR call or an ARS call that a system user originates, or routes over an incoming tie trunk can require a dialed authorization code to continue routing.

When you administer authorization codes, ensure that the user does not have to dial the authorization code more than once. For example, if a user makes an AAR call or an ARS call, and the FRL of the user is not high enough to access any of the trunks in the routing pattern, the system prompts the user for an authorization code. If the FRL that is assigned to the authorization

code is high enough to access the next trunk group in the routing pattern, the user is not prompted to dial the code again. If the system routes the call through another system, the user might be required to dial an authorization code again. This type of situation can be avoided through careful administration.

An authorization code might be required on some, but not all, trunk groups. In such cases, the system prompts for an authorization code when the originating FRL is not high enough to access the next available trunk group in the routing pattern.

Authorization codes with UDP calls

UDP calls do not prompt the caller for an authorization code because UDP calls are viewed as internal calls to the caller. If the caller does not have the required facilities restriction level (FRL) to route a UDP call to another Communication Manager server, the call fails and the caller receives Intercept Treatment.

If you use UDP to place calls to public network numbers, you can use the first digit that is usually reserved for the ARS Feature Access Code for other purposes. For example, in North America, this would free up the first digit 9. If you still want these UDP-dialed calls to be prompted for an Authorization Code, use ARS to route these UDP numbers and enable the parameter UDP-ARS Calls Considered Offnet on the Dial Plan Parameters screen.

Note:

Communication Manager will not prompt the caller for an authorization code if you route a UDP number using AAR.

Authorization Codes administration

The following tasks are part of the administration process for the Authorization Codes feature:

- Setting up Authorization Codes
- Creating Authorization Codes with a specific Class of Restriction

Related links

Setting up Authorization Codes on page 268
Creating Authorization Codes with a specific Class of Restriction on page 269

Preparing to administer Authorization Codes

Procedure

On the Optional Features screen, ensure that the **Authorization Codes** field is set to `y`.

If the **Authorization Code** field is set to n, your system is disabled for the Authorization Codes feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Authorization Codes, or to open a service request.

To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

Screens for administering Authorization Codes

Screen name	Purpose	Fields
Optional Features	Ensure that the Authorization Codes feature is enabled on the system.	Authorization Code
Feature-Related System Parameters	Enable the Authorization Codes feature, and set up other fields to administer the feature.	• Authorization Code Enabled • Authorization Code Length • Display Authorization Code
Authorization Codes - COR Mapping	Create an Authorization Code that has a specific COR.	• AC • COR
Trunk Groups	Allow the use of Authorization Code to access trunks.	• Auth Code

Setting up Authorization Codes

Procedure

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

   The system displays the Feature-Related System Parameters screen.

2. In the **Authorization Code Enabled** field, type `y` to enable the Authorization Codes feature on a system-wide basis.

3. In the **Authorization Code Length** field, type the number of digits that you want for the authorization code.

   This field defines the length of the Authorization Codes your users need to enter. To maximize the security of your system, Avaya recommends that authorization codes must have at least 4 digits, but no more than 13 digits.

4. In the **Authorization Code Cancellation Symbol** field, leave the default of the pound sign (#).

   Users must dial this symbol to cancel the 10-second wait period during which your user can enter an authorization code.

5. In the **Attendant Time Out Flag** field, leave the default of n.

   When you set this field to n, the system does not route a call to the attendant if a user does not dial an authorization code within 10 seconds, or a user dials an invalid authorization code.

6. In the **Display Authorization Code** field, type `n`.

   When you set this field to set to n, the authorization code does not display on the phone sets thus maximizing security.

7. Press `Enter` to save your changes.
8. Type `change authorization-code n`, where *n* is the authorization code. Press `Enter`.

   The system displays the Authorization Code - COR Mapping screen.
9. In the **AC** field, type the authorization code that your users must dial.

   The number of digits in the code that you type must be the same as the number you assigned in the Feature-Related System Parameters screen.
10. In the **COR** field, type a COR number from 0 through 95.
11. Press `Enter` to save your changes.

Creating Authorization Codes with a specific Class of Restriction

About this task

Using authorization codes, a caller can override the calling privileges. For example, you can give a supervisor an authorization code so that they can make calls from a telephone that is usually restricted for these calls. Since each authorization code has a Class of Restriction (COR), the system uses the COR that is assigned to the authorization code, and the FRL assigned to the COR to override the privileges associated with the restricted phone.

Authorization codes do not override dialed strings that are denied. For example, if your Automatic Route Selection (ARS) tables restrict users from placing calls to destinations that are outside of the country, a caller cannot override the restriction with an authorization code.

Procedure

1. Type `change authorization-code n`, where *n* is the authorization code. Press `Enter`.

   The system displays the Authorization Code - COR Mapping screen.
2. In the **AC** field, type the code that you want to use.
3. In the **COR** field, type the COR number.
4. Press `Enter` to save your changes.

Considerations for Authorization Codes

This section provides information about how the Authorization Codes feature behaves in certain circumstances. Use this information to ensure that you receive maximum benefits of the Authorization Codes feature under all conditions:

- From remote locations users usually access authorization from touch-tone telephones. However, users can also do so from rotary telephones at specified authorization-code-forced locations that follow appropriate trunk administration practices. Rotary station users access

attendants using Listed Directory Numbers (LDN) or Remote Access Numbers (RAN), and can experience a 10-second timeout.

- The use of Authorization Codes does not limit other call-control methods, such as Toll Restriction, Miscellaneous Trunk Restriction, and Outward Restriction.
- For security reasons, do not assign authorization codes in sequential order. Assign random number barrier codes and authorization codes to users. Random codes prevent hackers from deciphering the sequential codes.
- If timeout to attendant does not occur or a Cancellation of Authorization Code Request (CACR) digit codes are dialed instead of authorization codes, the system assumes that invalid authorization codes were dialed and the caller hears intercept tones.
- Authorization codes can have an impact calling privileges. Authorization codes can:
  - Change the FRL of an outgoing call when the FRL is not high enough to access preferred that AAR/ARS assigns. An FRL is assigned to a COR that is associated with user authorization codes. No additional COR data is assigned.
  - Overrides COR for remote access calls that are assigned to barrier codes, when required. if an authorization code is required for remote access calls, the user is assigned the COR of the dialed authorization code, with all connected data, such as the FRL. This COR overrides the COR that is assigned to any required barrier code.
  - Override the COR that is associated with a VDN, if an authorization code is required. The COR of the Authorization code is applicable on this call.

    The Authorization Code COR overrides the Barrier Code COR, the Barrier Code COR in turn overrides the VDN COR, and the VDN COR in turn overrides the COR of the originator.
- Incoming trunk calls that require authorization codes retain user privileges.

Interactions for Authorization Codes

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

AAR/ARS Partitioning

Class of Restriction (COR) assigns partitioned group numbers and authorization codes can change CORs. Therefore, authorization codes can change Partitioned Group Numbers on incoming remote access calls. For originating calls, the COR of the user determines Partitioned Group Numbers.

Cancellation of Authorization Code Request

If	Then
CACR =1	• Authorization = 1
Network = DEFG1, DEFG3 or DEF ECSR5	• CACR can be #
Network - S85s, DIM switch	• CACR = 1 (default)

COR and Facilities Restriction Level (FRL)

Authorization codes used for AAR or ARS calls override the associated FRL.

Associated Classes of Restriction determine remote-access user privileges.

Forced Entry of Account Codes and Call Detail Recording

For 94A LSU and 3B2 CDRU 18-word records, authorization codes are output if administered account-code lengths are fewer than six digits. For 59-character records, authorization codes are never recorded. Note that 94A LSU and 3B2 CDRU are no longer supported.

Authorization codes are recorded after destination addresses are dialed. Invalidly dialed authorization codes are recorded, and CDR printouts can be used to determine patterns.

Security Violation Notification

The system monitors and reports authorization code violations.

Chapter 41: Automated Attendant

Using the Automated Attendant feature, callers can dial an extension without the need for an attendant to connect the call.

Detailed description of Automated Attendant

A caller dials any extension on the system. The Automated Attendant feature uses vectors to route the call to that extension. This feature reduces the need for live attendants, which can help to reduce costs.

The Automated Attendant feature works together with the Attendant Vectoring feature. For more information, see the “Attendant Vectoring” feature. For more information about vectors and vector directory numbers (VDNs), see the “Meet-Me Conference” feature.

The *Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference* contains a detailed description of Automated Attendant, and how to use the Automated Attendant feature. The guide also gives a sample vector that you can use for Automated Attendant.

Automated Attendant administration

The following tasks are part of the administration process for the Automated Attendant feature:

- Setting the prompting timeout for Automated Attendant
- VDN administration for Automated Attendant
- Announcement administration for Automated Attendant
- Controlling hunt groups by vector for Automated Attendant
- Assigning a caller information button on a multiappearance telephone
- Assigning a caller information button on an attendant console

Related links

Setting the prompting timeout for Automated Attendant on page 273
VDN administration for Automated Attendant on page 274
Announcement administration for Automated Attendant on page 274
Controlling hunt groups by vector for Automated Attendant on page 274

Assigning a caller information button on a multiappearance telephone on page 275
Assigning a caller information button on an attendant console on page 275

Preparing to administer Automated Attendant

Procedure

1. Set up the attendant console.

   For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

2. On the Optional Features screen, ensure that the **Vectoring (Prompting)** field is set to `y`.

   If the **Vectoring (Prompting)** field is set to `n`, your system is not set up for the Automated Attendant feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Automated Attendant, or to open a service request.

   To view the Optional Features screen, type **`display system-parameters customer-options`**. Press `Enter`.

Screens for administering Automated Attendant

Screen name	Purpose	Fields
Optional Feature	Ensure that the Automated Attendant feature is activated.	Vectoring (Prompting)
Feature-Related System Parameters	Set the prompting timeout period.	Prompting Timeout
Vector Directory Number	Assign a VDN to an extension.	All
Announcements/Audio Sources	Complete all fields for each extension that provides an Automated Attendant announcement.	All
Hunt Group	Indicate that the system controls hunt groups with vectors.	Vector
Call Vector	Complete a Call Vector screen for each Automated Attendant vector.	All
Station	Assign a **callr-info** display button for multiappearance telephones.	Any blank field in either the **Button Assignments** area or the **Feature Button Assignments** area
Attendant Console	Assign a **callr-info** display button for attendant consoles.	Any blank field in the **Feature Button Assignments** area

Setting the prompting timeout for Automated Attendant

Procedure

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

2. On the Feature-Related System Parameters, click `Next` until you see the **Vectoring** area.
3. In the **Prompting Timeout (sec)** field, type the number of seconds before the **`collect digits`** command times out for callers who use rotary dialing.

   This value must be a number from 4 to 10. The default is 10.

   The Optional Features screen displays the **Prompting Timeout (sec)** field only if the **Vectoring (Prompting)** field is set to y.
4. Press `Enter` to save your changes.

VDN administration for Automated Attendant

To administer a vector directory number (VDN), see *Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*.

See also the Attendant Vectoring feature.

Related links

Attendant Vectoring on page 244

Announcement administration for Automated Attendant

To administer announcements for the Automated Attendant, see the Announcements feature.

Related links

Announcements on page 162

Controlling hunt groups by vector for Automated Attendant

Procedure

1. Enter `change hunt-group n`, where *n* is the number of the hunt group that you want to control by vector.
2. In the **Vector** field, type `y` to indicate that this hunt group is vector controlled.

   You can change the **Vector** field to `y` only if the **Vectoring (Basic)** field on the Optional Features screen is set to `y`. For more information on setting up hunt groups, see the Hunt Groups feature.
3. Select **Enter** to save your changes.

Related links

Hunt Groups on page 838

Assigning a caller information button on a multiappearance telephone

About this task

You can administer any multiappearance display telephone to have a caller information (**callr-info**) button. This button displays digits that were collected for the last **collect digits** command.

Procedure

1. Type `change station n`, where *n* is the extension of the telephone that you want to change. Press `Enter`.
2. On the Station screen, click `Next` until you see the **Button Assignments** area.

   If all the buttons are assigned in this area, click `Next` until you see the **Feature Button Assignments** area.
3. In the **Button Assignments** area or in the **Feature Button Assignments** area, assign `callr-info` to an available button.
4. Press `Enter` to save your changes.

Assigning a caller information button on an attendant console

About this task

You can administer an attendant console to have a caller information (**callr-info**) button. This button displays digits that were collected for the last **collect digits** command.

Procedure

1. Type `change attendant n`, where *n* is the number of the attendant console to which you want to assign a **callr-info** button. Press `Enter`.
2. On the Attendant Console screen, click `Next` until you see the **Feature Button Assignments** area.
3. In the **Feature Button Assignments** area, assign `callr-info` to an available button.
4. Press `Enter` to save your changes.

Considerations for Automated Attendant

This section provides information about how the Automated Attendant feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Automated Attendant under all conditions.

Interactions for Automated Attendant

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

Authorization Codes

The system does not prompt for an authorization code, and the **route-to** command fails if:

- Authorization codes are enabled
- A **route-to** command in a prompting vector accesses either Automatic Alternate Routing (AAR) or Automatic Route Selection (ARS)
- The Facility Restriction Level (FRL) of the vector directory number (VDN) cannot use the chosen routing preference

CallVisor Adjunct-Switch Application Interface (ASAI)

The Call Vectoring feature can collect ASAI-provided digits through the **collect vector** command as dial-ahead digits. The system passes CINFO to CallVisor ASAI.

Hold

If a call is put on hold during the processing of a collect command, the command restarts at the announcement prompt when the call is taken off hold. All dialed-ahead digits are lost. Similarly, if a call to a vector is put on hold, vector processing is suspended when a collect command is encountered. When the call becomes active, the collect command resumes.

Inbound Call Management (ICM)

You can use Automated Attendant to collect information that an adjunct might later use to handle a call.

Transfer

If a call to a VDN is transferred during a collect command, the collect command restarts when the transfer is complete. All dialed-ahead digits are lost. Similarly, if a call to a vector is transferred, vector processing is suspended when a collect command is encountered. When the transfer is complete, the collect command resumes. Attendant-extended calls suspend vector processing in the same way as transferred calls.

Chapter 42: Automatic Callback

Using the Automatic Callback (ACB) feature, internal users who place a call to a busy or an unanswered internal telephone can be called back when the called telephone becomes available.

Detailed description of Automatic Callback

When the caller makes a call to a busy or an unanswered internal telephone, the system calls the caller when the called party becomes available. Upon hearing the busy signal, the caller activates the Automatic Callback feature and disconnects the call. The system monitors the called party. When the called party becomes available to receive the call, the system automatically initiates the Automatic Callback call. The caller receives priority ringing. The caller then lifts the handset, and the called party receives the same ringing that the system provided on the originating call.

For example, Station A calls Station B. Station B is busy or not answering. Station A sets the Automatic Callback feature. When Station B becomes available, the system will call Station A. This is ringout call. The system does not present the ringout call to Station A pickup group or bridges. Once Station A answers, the system rings Station B. This is callback call. Callback call is like a normal call made to Station B and can be picked up by Station B pickup group or bridges.

To activate the Automatic Callback feature, the user of a single-line telephone presses the **Recall** button, or flashes the switchhook. The user then dials the Automatic Callback Feature Access Code (FAC). A single-line user can activate Automatic Callback for only one call at a time.

When you place a call from an analog telephone, and the line is busy, an announcement prompts you to either:

- Enter the digit 1 to activate Automatic Callback.
- Enter the digit 2 to route the call to a hunt group extension.

The number of calls for which a user of a mult-iappearance telephone can activate Automatic Callback depends on the number of Automatic Callback buttons that you assign to the telephone. After the user places a call to a telephone that is busy or unanswered, the user presses an idle Automatic Callback button, and hangs up.

If the original caller answers an Automatic Callback call, and for some reason the called extension cannot accept the Automatic Callback call, the caller hears a confirmation tone and then silence. The call is still queued.

Users cannot activate Automatic Callback for calls to:

- A telephone that is assigned Termination Restriction
- An extension toward which Automatic Callback is already activated

  Note:

  This is overridden if **Automatic Callback With Called Party Queueing** is set as `y`.
- A data terminal or a data module
- An attendant console group
- A Terminating Extension Group (TEG)
- An extension for a hunt group, a split, or a skill
- The login ID of an EAS agent
- A Vector Directory Number (VDN) extension
- A forwarded called party to a station which in turn is forwarded to another station.

Ringback Queuing

You can administer your system to call users back if users try to place an outgoing call over a trunk group when all trunks are busy. Ringback Queuing places outgoing calls in an ordered queue (first-in, first-out) when all trunks are busy. The system automatically places the callback call to the telephone when a trunk becomes available, and the user hears a distinctive three-burst signal, which indicates an Automatic Callback call from the system. When the user answers the callback call, the original call automatically continues. Redialing is not required. Ringback queuing is also called Automatic Callback for busy trunks.

If a user with a multiappearance telephone has an idle **Automatic Callback** button and tries to access an all-trunks-busy trunk group, the call queues automatically. The lamp that is associated with the **Automatic Callback** button lights, and the user hears a confirmation tone.

Important:

Automatic Callback applies to stations. Ringback Queuing provides the same function for calls directed to a busy trunk group.

Ringback Queuing is automatic for a single-line telephone. After dialing is complete, the user hears a confirmation tone if the queue is available. No action is required. The system queues calls based on the value in the **Queue Length** field on the Trunk Group screen. The system checks the busy or idle status of the trunk group only once. If all trunks are busy, the call queues, even if a trunk has become available by the time that the caller finishes dialing. In this case, a caller might be called back immediately after the caller receives a confirmation tone and hangs up.

You can specify queuing for any outgoing-only trunk group that is not part of a distributed communications system (DCS), or for the outward direction of a non-DCS two-way trunk group.

Called Party Queuing

From Communication Manager Release 5.2, using Automatic Callback you can queue called parties. This feature works on analog, DCP, IP (H.323) and IP (SIP) telephones. From Communication Manager Release 5.2 onwards, use Automatic Callback for:

- Multiple active callbacks for an extension, subject to the limitation on the total number of callbacks within the system
- Callbacks for softphones, provided the softphone has at least one bridged call appearance on a physical station

A called telephone can have multiple active automatic callbacks. The callbacks are processed in the order in which they were activated. For the SIP endpoint only one automatic callback call is queued. The latest ACB activation overrides the previous queued call.

If a calling station uses multiple call appearances, the number of automatic callbacks depends on the number of Automatic Callback buttons assigned to the station.

Automatic Callback works the same way as it does on a local server, on the following networks:

- On a Distributed Communication Server (DCS) network, Automatic Callback (ACB) requests from or to a station located on a different Communication Manager are queued and processed.
- If your public service network provider supports ISDN Call Completion Busy Subscriber (CCBS), the CCBS requests are queued and processed.
- On a QSIG network, ACB requests from or to a station located on a different Communication Manager are queued.

Analog Busy Automatic Callback Without Flash

With Analog Busy Automatic Callback Without Flash, callers who place a call from an analog station to a station that is busy and has no coverage path or forwarding, hear an announcement and are presented with options. Depending on the selection that the caller makes, the call is queued to Automatic Callback, routed to an extension, or dropped. No switchhook flash is required for Analog Busy Automatic Callback.

QSIG Call Completion - Administrable TSC Signaling Connection

This capability covers auto callback within a private corporate network only, for example, through QSIG. Communication Manager Release 4.0 or later provides an administrable option on the Trunk Group screen for users to specify the method of signaling connection the system uses while waiting for a busy station to become idle.

Using the **TSC Method for Auto Callback** field on the QSIG Trunk Group Options page of the Trunk Group screen, customers can administer whether or not to retain the Temporary Signaling Connection (TSC) when QSIG Call Completion (QSIG-CC) is activated with other Communication Manager servers, or with non-Communication Manager servers (like the I55 or Siemens Hicom). The default value for the **TSC Method for Auto Callback** is drop-if-possible. The other option is to set the value to always-retain.

Older QSIG-CC standards require Path Reservation, which is not supported by Communication Manager. QSIG-CC can fail if the QSIG TSC is dropped when connected to a server that does not support the latest version of the QSIG-CC standards. In order for Communication Manager to work with servers based on old QSIG-CC standards, this retaining option is needed.

Currently, the preferred QSIG-CC signaling connection method used by Communication Manager is the signaling connection release. In other words, Communication Manager populates the element retain-sig-connection in CCBS/CCNR invoke APDUs with the hard-coded value FALSE. With Communication Manager 4.0 or later, the new administration option on the Trunk Group screen controls:

- the element retain-sig-connection in CCBS/CCNR invoke APDUs, when Communication Manager is the originating PINX
- the signaling connection method for the QSIG-TSC when Communication Manager is the terminating or the outgoing gateway PINX

For more information, see *Avaya Aura® Communication Manager Screen Reference*.

ISDN CCBS Supplementary Service on Busy

In EMEA, the public network service providers support the ISDN Call Completion Busy Subscriber (CCBS) capabilities where the service provider allows Automatic Callback for a busy subscriber. By implementing ISDN CCBS Supplementary Services, Communication Manager enables automatic callback to the public network from release 5.0 onwards.

Note:

The CCBS feature is not supported by all service providers. The Call Completion on No Reply (CCNR) feature is defined by the ETSI standards. But the CCNR feature is not supported by Communication Manager, or by service providers for new customers.

The following settings must be administered to use this feature:

1. On the ISDN Trunk Group screen, set **Supplementary Service Protocol** to option `c` (which is usually already set for ETSI public network trunks).
2. Also on the ISDN Trunk Group screen, set **NCA-TSC Trunk Member** to the trunk member whose D-channel will be used to route the ETSI CCBS request.
3. To enable ETSI for BRI, you must set the **Interface** column to `user` or `network` to enable option `c` (stated in step 1) in the TSC SS Protocol column on the BRI-Trunk-Board screen. Also, the maximum number for the **NCA-TSC** field has to be a value > 0.
4. For PRI, you must set the **TSC Supplementary Service Protocol** field on the Signaling Group screen to `c` to enable ETSI. Also, the maximum number of **NCA-TSC** field on the Signaling Group screen has to be set to a value > 0.

For more information, see *Avaya Aura® Communication Manager Screen Reference*.

CCBS for Incoming Calls

The Call Completion to Busy Subscriber (CCBS) feature is based on the existing auto callback and supplementary service - completion of calls (QSIG SS-CC) features. It provides the auto

callback functionality to be used on calls to or from the public network. The server informs the caller as soon as the busy subscriber becomes available.

This feature supports the following:

- ETSI-TSC (Temporary Signaling Connection) for incoming calls. In Communication Manager Release 5.0 and earlier releases, TSC is available for ETSI only for outgoing calls. TSC is currently available in both directions for QSIG.
- ETSI-CCBS for incoming calls. In Communication Manager Release 5.0 and earlier releases, CCBS is only fully available for internal users and for users on systems interconnected by DCS, QSIG, or SIP trunks. On the ETSI interface, CCBS is supported for outgoing calls only. Starting with Communication Manager Release 5.1, CCBS on the ETSI interface is fully available in both directions (incoming and outgoing).

Restriction: ETSI-TSC and ETSI-CCBS are implemented without gateway functionality (ETSI - QSIG/DCS/SIP).

The supplementary service Completion of Calls has been added as new ETSI ISDN functionality. This feature is supported only in countries where the ETSI ISDN protocol is supported.

This feature must be supported by the service provider. Some service providers offer Call Completion without any additional charge, but you need to apply for it.

Completion of Calls is known as “Auto callback” at the user side.

CCBS Call Flow Scenarios

As an analog voice terminal user, you can activate supplementary service - Call Completion to Busy Subscriber (SS-CCBS) by pressing the **Recall** button or flashing the switch hook, then dialing the Automatic Callback Activation Feature Access Code. You can activate only one Automatic Callback call at any given time.

As a multi-appearance voice terminal user, you can activate SS-CCBS for the number of Automatic Callback buttons assigned to the terminal. After placing a call to a voice terminal over the DSS1 network that is busy, you can activate SS-CCBS by pressing an idle Automatic Callback button.

In the above two scenarios, the called station is located in the public network. The public network access must be located in the same switch as the station.

When you request a CCBS supplementary service it remains active until the Call Completion is performed or until the Service Duration timer expires. The default for the timer is set to 40 minutes. The terminal must be located in the same switch as the public network access.

When SS-CCBS is activated towards the busy station on the terminate side (public network or PBX), the terminating side monitors the called voice terminal. When the called voice terminal becomes available to receive a call, the terminating side notifies the originating side of the possibility of executing a Call Completion call attempt. The originating side then originates the Call Completion call.

A busy voice terminal becomes available when the user hangs up after completing the current call.

A SS-CCBS request is canceled for any of the following user-related reasons:

- The Call Completion call is successful.
- The called party at the terminating PBX is unavailable within 40 minutes.
- The called party is busy again.

CCBS Routing issue

CCBS requests using the ETSI ISDN network require a special view to the routing in Communication Manager. It might be necessary to add an additional routing entry for an incoming ETSI CCBS request to reach the dedicated station.

In an incoming ETSI basic call, the called number is always supplied by the network provider. With CCBS, the called number is supplied by the requesting user. If the requesting user encodes the number in a different way than the network provider does, CCBS will fail. In this case, an additional routing entry is necessary for the ETSI CCBS request to reach the called number.

For example, station 7001 has a PBX access code of 53608. The national destination code (also known as the city code) is 211.

On an incoming basic call, the called number may be presented as 536087001. In this example, the call can be routed to the dedicated station because 53608 is configured in the ars digit-conversion table.

In an incoming ETSI CCBS request, the called number may be presented as 211563087001. Keep in mind this number is provided by the requesting user, not by the network provider. The CCBS request will fail if only 53608 is entered in the ars digit-conversion table. To make CCBS work, the digit sequence 21153608 must be added to the ars digit-conversion table.

The figure on page 282 shows the entries for this example:

```
display ars digit-conversion 0                                  Page 1 of 2
                     ARS DIGIT CONVERSION TABLE
                               Location: all                Percent Full: 0

  Matching Pattern    Min   Max   Del   Replacement String   Net    Conv ANI Req

  53608               5      9    5                          ext    n        n
  21153608            8     12    8                          ext    n        n
```

Figure 2: ars digit-conversion table

Automatic Callback administration

The following tasks are part of the administration process for the Automatic Callback feature:

- Assigning a FAC for Automatic Callback
- Enabling Automatic Callback With Called Party Queuing

- Setting the no-answer timeout interval for Automatic Callback
- Assigning a feature button for Automatic Callback
- Setting the Queue length for Ringback Queuing
- Enabling CCBS

Related links

[Assigning a FAC for Automatic Callback](#) on page 283
[Enabling Automatic Callback with Called Party Queuing](#) on page 284
[Setting the no-answer timeout interval for Automatic Callback](#) on page 284
[Assigning a feature button for Automatic Callback](#) on page 284
[Setting the queue length for Ringback Queuing](#) on page 284
[Enabling CCBS](#) on page 285

Screens for administering Automatic Callback

Screen name	Purpose	Fields
Feature Access Code (FAC)	Assign a Feature Access Code (FAC) with which to activate or deactivate Automatic Callback.	Automatic Callback Activation/ Deactivation
Feature-Related System Parameters	Set the number of times that the callback call rings at the calling station before the system cancels the callback call.	Automatic Callback With Called Party Queuing-No Answer Timeout Interval
Station (multiappearance)	Assign a feature button for the Automatic Callback feature.	Buttons/Feature Button Assignments - auto-cback
Trunk Group	Set the queue length for Ringback Queuing.	Queue Length
	Enable CCBS	Supplementary Service Protocol NCA-TSC Trunk Member

Assigning a FAC for Automatic Callback

Procedure

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

   The system displays the Feature Access Codes (FAC) screen.
2. In the **Automatic Callback Activation** field, type the digits of the access code that you want to use to activate the Automatic Callback feature.
3. In the **Deactivation** field, type the digits of the access code that you want to use to deactivate the Automatic Callback feature.
4. Press `Enter` to save your changes.

Enabling Automatic Callback with Called Party Queuing

Procedure

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

   The system displays the Feature-Related System Parameters screen.
2. Set **Automatic Callback With Called Party Queuing** to `y`.
3. Press `Enter` to save your changes.

Setting the no-answer timeout interval for Automatic Callback

Procedure

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

   The system displays the Feature-Related System Parameters screen.
2. In the **Automatic Callback - No Answer Timeout Interval (rings)** field, enter the number of times that you want a callback call to ring at the calling station before the callback call is canceled.
3. Press `Enter` to save your changes.

Assigning a feature button for Automatic Callback

Procedure

1. Type `change station` *n*, where *n* is the extension of the station for which you want to assign a feature button.

   If you are adding a new station, type `add station next`.

   The system displays the Station screen.
2. In the **Button Assignments** area, type `auto-cback` in a blank field.
3. Repeat Step 2 for as many buttons as you want to assign for Automatic Callback.
4. Press `Enter` to save your changes.

Setting the queue length for Ringback Queuing

Procedure

1. Type `change trunk-group` *n*, where *n* is the number of an existing trunk group for which you want to set the queue length.

   If you are adding a new trunk group, type `add trunk-group next`.

   The system displays the Trunk Group screen.
2. In the **Queue Length** field, type the number of outgoing calls that you want to be held waiting when all trunks are busy.

3. Press `Enter` to save your changes.

Enabling CCBS

Procedure

1. Set the **Supplementary Service Protocol** field on Page 2 of the Trunk Group screen to `c`.
2. Set the **NCA-TSC Trunk Member** field on Page 3 of the Trunk Group screen.

Considerations for Automatic Callback

This section provides information about how the Automatic Callback feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Automatic Callback under all conditions. The following considerations apply to Automatic Callback:

- The system cancels an Automatic Callback request if the:
  - Called party is unavailable within 30 minutes.
  - Calling party does not answer the callback call within the administered interval. This interval consists of two to nine ringing cycles, and is set in the **Automatic Callback-No Answer Timeout Interval** field on the Feature-Related System Parameters screen.
  - Calling party decides not to wait, and presses the same **Automatic Callback** button a second time on a multiappearance telephone, or dials the Automatic Callback cancellation code on a single-line telephone.
- In the Change off-pbx-telephone configuration-set screen, if you set the **Fast Connect on Origination?** field to `y`, then the automatic callback does not work.
- Automatic Callback is administered for individual telephones by Class of Service (COS), and cannot be assigned to attendants. Multiappearance telephones must have an **Automatic Callback** button to activate the feature.
- Automatic Callback works differently, depending on whether the called party is busy or does not answer the call. For a busy call, Automatic Callback occurs as soon as the called party hangs up. For an unanswered call, the telephone must be used for another call, and then hung up before Automatic Callback occurs.

  Note:

  If the user who originates an Automatic Callback originator has all line appearances occupied when the Automatic Callback call comes in, the user hears priority ringing once, and the Automatic Callback lamp blinks. However, if the user presses the **Automatic Callback** button to answer the Automatic Callback call, the system drops one of the other calls.
- Queuing can reduce the number of trunks that are required.
- On a multiappearance telephone, one callback call can be associated with each **Automatic Callback** button that is assigned to the terminal.

- On a single-line telephone, only one Automatic Callback call can wait at a time.
- Queue requests are canceled when:
  - A trunk is unavailable within 30 minutes.
  - The user does not answer the callback call within the administered interval.
  - The telephone is busy when the callback call is attempted.
  - The user dials the Ringback Queuing cancellation code, or presses the **Automatic Callback** button that is associated with the queued call.
- Incoming tie-trunk calls cannot queue on an outgoing trunk group. The system does not know the calling number, and cannot originate the callback call.
- The system checks the busy or idle status of the trunk group only once. If all trunks are busy, the call queues, even if a trunk becomes available by the time that the caller finishes dialing. In this case, a caller might be called back immediately after the caller receives a confirmation tone and hangs up.
- A trunk might appear to be available, yet outgoing calls are queued. The trunk is not free, because the trunk is reserved for a previous Automatic Callback request.
- The Automatic Callback feature works correctly even if each of the call's parties is using a SIP endpoint administered on and managed by a different instance of Communication Manager.

Interactions for Automatic Callback

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

Attendant Call Waiting and Call Waiting Termination

If a user activates Automatic Callback to or from a single-line telephone, Call Waiting Termination is denied.

Attendant Intrusion

Attendant Intrusion does not work if a user has activated Automatic Callback.

Automatic Route Selection (ARS)

If a user with a multiappearance telephone that has an Automatic Callback button makes an ARS call, and all trunks are busy, the system activates Ringback Queuing automatically.

Bridged Call Appearance

Users cannot activate Automatic Callback from a bridged call appearance. If a user activates Automatic Callback from a primary extension number, the return-call notification rings at all bridged call appearances.

Busy Verification

If a user has activated Automatic Callback on a telephone, you cannot perform Busy Verification of that telephone.

Call Coverage

If the calling station has Call Coverage active, the callback terminates at the called station and does not follow the coverage path.

Call Forwarding

If the calling party has activated Call Forwarding on a telephone, the calling party is able to activate Automatic Callback. If the called party activates Call Forwarding on a telephone before the caller trying to use Automatic Callback, the calling party is unable to activate Automatic Callback. Also, if Automatic Callback was activated before the called telephone user activated Call Forwarding, the system redirects the callback call attempt toward the callback party, not to the forwarded-to party.

- If the calling station has Call Forwarding active, the callback is forwarded only if the forwarded station is local to the calling station. You cannot activate Automatic Callback if the forwarded station is remote to the calling station.
- If a forwarded station that has active automatic callback has any activity going on, callback is not generated till one of the following conditions is met:
  - the forwarded station goes on hook
  - the forwarding is removed and the user goes on and off hook
- Automatic callback cannot be activated if the called party is forwarded to a station that is forwarded to another station.

Call Pickup

A pickup group member cannot answer a ringout call. For information on ringout call and callback call see Detailed description of Automatic Callback on page 277.

Class of Restriction (COR)

Telephones with origination restriction cannot activate Automatic Callback.

Conference and Transfer

A user of a single-line telephone can activate conference or transfer if Automatic Callback is activated.

Distributed Communication System (DCS)

Automatic Callback operates over a DCS network in the same way that Automatic Callback operates on a local server.

Expert Agent Selection (EAS)

Users cannot activate Automatic Callback to the login ID of an EAS agent. Users can activate Automatic Callback to the telephone where the agent is logged in.

Hold

A user of a single-line telephone cannot receive Automatic Callback calls if the user has placed a call on hold.

Hot Line Service

Telephones that are administered for Hot Line Service cannot activate Automatic Callback.

Intercom - Automatic and Dial

Intercom calls are ineligible for Automatic Callback.

Internal Automatic Answer (IAA)

IAA does not automatically answer Automatic Callback calls.

Manual Originating Line Service

Telephones with Manual Originating Line Service cannot activate Automatic Callback.

Personal Station Access

You cannot activate automatic callback to a disassociated PSA extension unless that extension is bridged to another physical station. If callback was activated before the disassociation, the callback remains in queue till the activation timer expires or the callback is explicitly canceled.

You cannot activate automatic callback from a disassociated PSA extension.

Public Network Trunks

Automatic Callback works on outgoing public network trunks in some countries. The call must be dialed using AAR, ARS, or UDP. Automatic Callback cannot be activated on a public network trunk call if the call was dialed using a Trunk Access Code (TAC).

QSIG

Automatic Callback operates over a QSIG network in the same way as on a local server. The call must be dialed using AAR, ARS, or UDP. Automatic Callback cannot be activated on a QSIG call if the call was dialed using a Trunk Access Code (TAC).

Remote Access

Callback calls cannot be made to Remote Access users, because the system does not know the calling number.

Ringback Queuing

Users can press an Automatic Callback button to activate Ringback Queuing.

Send All Calls

You cannot activate automatic callback on a station that uses the Send All Calls redirection option.

Telephone Display

When the system generates an Automatic Callback call, the display of the originating telephone displays Automatic Callback, or the equivalent translated phrase for Administrable Language Displays.

Limitations of Automatic Callback

Back-to-back Automatic Callback activation for the same remote station must have an interval of 32 seconds. This limitation of 32 seconds interval applies only when Automatic Callback is invoked remotely over a SIP trunk. It does not apply when Automatic Callback is invoked by using QSIG or Distributed Communication System (DCS).

However, this limitation is not applicable to back-to-back Automatic Callback activation for an internal station.

Chapter 43: Automatic Circuit Assurance

Use the Automatic Circuit Assurance (ACA) feature to identify possible trunk malfunctions. When you enable ACA, the system measures the holding time of each trunk call. If the measurements show calls with either extremely long or extremely short holding times, Communication Manager places a referral call to an attendant or a telephone.

Detailed description of Automatic Circuit Assurance

The system records the holding time from when a trunk is accessed to when the trunk is released. You set short and long holding-time limits for each trunk group. The system then compares the recorded holding times against these limits.

You enable ACA for the entire system, and administer thresholds for individual trunk groups. You can measure all trunks, or only certain trunks.

Communication Manager deals with long-holding and short-holding calls differently. For every call that is shorter than the administered short holding time, the system increases the short-holding counter by one. For calls over the same trunk that are within the normal range, the system decreases the short holding counter by one. Thus, trunks that handle a normal variety of call lengths are not singled out as faulty. If the counter reaches the administered short holding limit, the system places a referral call.

If one long call exceeds the long holding time, the system makes a referral call.

You cannot measure personal central office (CO) lines, out-of-service trunks, or trunks that are undergoing maintenance testing.

The ACA referral call

An ACA call includes a display message or a voice-synthesized message that states:

- That this call is an ACA call
- The access code, the trunk group number, and the trunk group member number
- The type of referral, either short holding time or long holding time

If the referral call is answered, the system displays this information until the call is released. If the call is unanswered within 3 minutes, the system ends the call. The system places the call again after one hour, and continues to place the call hourly until someone answers.

The attendant or the telephone user who receives the referral call can press the **aca-halt** button to stop further calls. The **aca-halt** button is a toggle button, and turns off the ACA feature until the user presses the button again.

The ACA audit trail

When the system makes a referral call, the system also adds a record to an audit trail. Audit trail records are available on the ACA Measurements Report. Each record contains the:

- Time and the date of referral
- Trunk group number, the trunk access code, and the trunk group member
- Type of referral, either short holding time or long holding time

Automatic Circuit Assurance administration

This section describes the screens for the Automatic Circuit Assurance feature.

Screens for administering Automatic Circuit Assurance

Screen name	Purpose	Fields
Feature-Related System Parameters	Enable the ACA feature	• Automatic Circuit Assurance Enabled • ACA Referral Calls • ACA Referral Destination • ACA Short Holding Time Originating Extension • ACA Long Holding Time Originating Extension
Trunk Features	Set assignments and thresholds	• ACA Assignment • Short Holding Threshold • Long Holding Time (hours) • Short Holding Time (seconds)
Attendant Console	Set the **aca-halt** feature button	Any available button in the **Feature Button** area
Station	Set the **aca-halt** feature button	Any available button in the **Feature Button** area

Reports for Automatic Circuit Assurance

The following reports provide information about the Automatic Circuit Assurance (ACA) feature:

- The ACA Measurements Report shows the audit trail for ACA calls.

For detailed information on these reports and the associated commands, see *Avaya Aura® Communication Manager Reports*.

Interactions for Automatic Circuit Assurance

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

Administrable Language Displays

You cannot administer languages for ACA messages.

Communication Manager Messaging

Do not set the referral-call extension to a telephone that covers to a Communication Manager Messaging voice messaging system. You can overload Communication Manager Messaging with the volume of calls, because ACA calls remain active for up to three minutes.

Busy Verification

Once you identify a potentially defective trunk, you can use Busy Verification to check that trunk.

Centralized Attendant Services (CAS)

When CAS is activated, the referral-call destination must be on the local switch. The system interprets a referral destination of 0 as the local attendant, if a local attendant exists. The CAS attendant cannot activate or deactivate ACA referral calls at a branch location.

Distributed Communications System (DCS)

Referral calls can be placed across a DCS network. The primary switch is administered to receive ACA referred calls from remote nodes for all switches within the network. You must administer the **ACA Remote PBX Identification** field on the Feature-Related System Parameters screen with the PBX ID of the node that is designated as primary.

If ACA referral calls are sent off the switch that generates the referral, the display and voicing information that indicates the failed trunk is lost, even if the referral call is made over a DCS network.

Night Service

The system does not place referral calls to the attendant if the system is in Night Service mode.

Visually Impaired Attendant Service (VIAS)

If the attendant presses the **Display Status** button and an ACA call has not been answered, the words “Automatic Circuit Assurance” are voiced.

If a visually-impaired attendant presses the **Display Status** button and the ACA call has been answered, the words Automatic Circuit Assurance and the extension that is assigned to the ACA call are voiced.

If the switch contains a voice-synthesis board, ACA referral calls are also accompanied by an audible message that identifies the type of ACA infraction encountered. The message is “Automatic circuit assurance <long> or <short> holding time threshold has been exceeded for trunk group <#> member number <#>.”

Voice Message Retrieval

If you use Voice Message Retrieval, you can assign a non-display telephone as a referral destination.

Wideband Switching

ACA treats wideband-trunk calls as a single-trunk call, and therefore triggers a single referral call. The call information shows the lowest B-channel trunk member that is associated with the wideband channel.

Chapter 44: Automatic Number Identification

Use the Automatic Number Identification (ANI) feature to display telephone number of the calling party on your display telephone. The system uses ANI to interpret calling party information that is signaled over multifrequency (MF) or Session Initiation Protocol (SIP) trunks.

Detailed description of Automatic Number Identification

ANI displays calling party information on your display telephone that is signaled over MF or SIP trunks.

- For a description about calling party information that is signaled over ISDN or H.323 trunks to your display telephone, see the “Caller ID” feature.
- For a description about calling party information that is signaled over Centralized Automatic Message Accounting (CAMA) trunks to your local emergency rapid response organization, see the “E911” feature.

Incoming Automatic Number Identification

Use inband signaling for information, such as the address digits for the called party, that is delivered over the same trunk circuit that is used for the voice or data connection. Use out-of-band or ISDN signaling when signaling information passes through a different signaling path than the path that is used for the voice or data connection.

For example, when a call is made from 555-3800 to your display telephone at extension 81120, and the **Incoming Tone (DTMF) ANI** field is set to *ANI*DNIS* on the Trunk Group screen, your trunk group receives *5553800*81120*. If the same field is set to ANI*DNIS*, your trunk group receives 5553800*81120*. In both cases, your telephone displays call from 555-3800.

Your telephone displays the incoming trunk group name if you do not use inband ANI.

Outgoing Automatic Number Identification

Outgoing ANI applies to outgoing Russian MF ANI, R2-MFC ANI, China #1 MF ANI, and Spain Multi Frequency España (MFE) ANI trunks only.

Use Outgoing ANI to specify the type of ANI to send on outgoing calls. You can define MF ANI (the calling party number, sent through multifrequency signaling trunks) prefixes by COR. Using this feature, a system can send different ANIs to different central offices (COs).

For a tandem call that uses different types of incoming and outgoing trunks, the server uses:

- The COR-assigned call type of the incoming trunk for Russian or R2-MFC outgoing trunks
- Automatic Route Selection (ARS) call types for MFE outgoing trunks

Automatic Number Identification administration

The following tasks are part of the administration process for the Automatic Number Identification (ANI) feature:

- Setting up ANI on a multifrequency trunk
- Displaying incoming ANI calling party information
- Outgoing ANI setup
- Setting up an ANI request button

Related links

Setting up ANI on a multifrequency trunk on page 296
Displaying incoming ANI calling party information on page 296
Outgoing ANI setup on page 297
Setting up an ANI request button on page 298

Screens for administering Automatic Number Identification

Screen name	Purpose	Fields
Multifrequency-Signaling-Related Parameters	Set up ANI on an MF trunk.	• Incoming Dial Type • Incoming Tone (DTMF) ANI
Trunk Group	Set up incoming ANI so that the system displays the calling party information from either an MF or a SIP trunk.	• Incoming Dial Type • Incoming Tone (DTMF) ANI
• AAR Digit Analysis Table • ARS Digit Analysis Table • AAR Digit Conversion Table • ARE Digit Conversion Table	Set up outgoing ANI for Russian MF ANI, R2-MFC ANI, China #1 MF ANI, and Spain Multi Frequency España (MFE) ANI trunks.	• ANI Reqd • ANI Req
Station	Assign an **ani-requst** button to the telephone of a user.	Any available button field in the **Button Assignments** area.

Setting up ANI on a multifrequency trunk

About this task

Using an ANI request button on the telephone, the user can display the telephone number of the calling party during the voice state of the call. The trunk must support this functionality.

Procedure

1. Type `change multifrequency-signaling n`, where *n* is a number between 1 and 8. Press `Enter`.

   The system displays the Multifrequency-Signaling-Related Parameters screen.

   Note:

   The number of pages and the fields on the screen that the system displays is based on the value in the **Outgoing Call Type** field.

   - If the value in the **Outgoing Call Type** field is group-ii-mfc, the system displays four pages. The system also displays the **ANI Prefix**, **Default ANI**, **Next ANI Digit Incoming**, and **Next ANI Digit Outgoing** fields.
   - If the value in the **Outgoing Call Type** field is mfe, the system displays two pages. The system also displays the **ANI Prefix**, and **Default ANI** fields.
   - If the value in the **Outgoing Call Type** field is none, the system displays three pages. The system also displays the **Next ANI Digit Incoming** field.

     For a thorough description of the Multifrequency-Signaling-Related Parameters screen and the values for the fields see the Administering *Avaya Aura® Communication Manager*.

2. When you are finished, press `Enter` to save your changes.

Displaying incoming ANI calling party information

About this task

A display telephone might display either the telephone number and name of the calling party, or the incoming trunk group name. You set the **ANI** field on the Trunk Group screen.

Procedure

1. Type `change trunk group n`, where *n* is the number of the trunk that you want to change. Press `Enter`.
2. On the Trunk Group screen, click `Next` until you see the **Incoming Dial Type** field.
3. In the **Incoming Dial Type** field, type `tone`.
4. Click `Next` until you see the **Incoming Tone (DTMF) ANI** field.
5. In the **Incoming Tone (DTMF) ANI** field, type `*ANI*DNIS`.

Note:

The system displays the `Incoming Tone (DTMF) ANI` field only when the **Incoming Dial Type** field on the previous page is set to `tone`.

6. Press `Enter` to save your changes.

Outgoing ANI setup

Preparing to set up outgoing ANI

Procedure

1. To view the Feature-Related System Parameters screen, type `change system-parameters features`. Press `Enter`.
2. Click `Next` until you see the **Allow ANI Restriction on AAR/ARS** field.
3. Ensure that the **Allow ANI Restriction on AAR/ARS** field is set to `y`.
4. Press `Enter` to save your changes.

Setting up outgoing ANI for AAR

Procedure

1. Type `change aar analysis`. Press `Enter`.

   The system displays the AAR Digit Analysis Table screen.

   Note:

   The system uses AAR routing information to route calls within your company over your own private network. The software converts the number that the user dials. The software then analyzes the number, and routes the call as a private-network call.

2. For each appropriate dialed string on your plan, set the **ANI Reqd** field.
3. Press `Enter` to save your changes.
4. Type `change aar digit-conversion`. Press `Enter`.

   The system displays the AAR Digit Conversion Table screen.

5. For each appropriate Replacement string, set the **ANI Reqd** field.
6. Press `Enter` to save your changes.

Setting up outgoing ANI for ARS

Procedure

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

   The system displays the ARS Digit Analysis Table screen.

Note:

The system uses ARS routing information to route calls that go outside your company over public networks. The system also uses ARS routing information to route calls to remote company locations if you do not have a private network. The software converts the number that the user dials. The software then analyzes the number, and routes the call as a public network call.

2. For each appropriate dialed string on your plan, set the **ANI Reqd** field.
3. Press `Enter` to save your changes.
4. Type `change ars digit-conversion`. Press `Enter`.

   The system displays the ARS Digit Conversion Table screen.
5. For each appropriate Replacement string, set the **ANI Reqd** field.
6. Press `Enter` to save your changes.

Setting up an ANI request button

About this task

Using an ANI request button on the telephone, the user can display the telephone number of the calling party during the voice state of the call. The trunk must support this functionality.

Procedure

1. Type `change station` *n*, where *n* is the extension that you want to change. Press `Enter`.
2. On the Station screen, click `Next` until you see the **Button Assignments** area.
3. In an available button field, type `ani-requst`.
4. Press `Enter` to save your changes.

Interactions for Automatic Number Identification

This section provides information about how the Automatic Number Identification (ANI) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of ANI in any feature configuration.

Attendant Console

If an attendant extends a call, the attendant's Class of Restriction (COR) is used to select the ANI prefix.

Authorization Codes

The authorization code COR is used to select the ANI prefix. The extension's ANI is used if an extension originates the call. The ANI for the server is used if the originating endpoint is an incoming MF or SIP trunk.

Bridged Call Appearance

A call from a bridged call appearance uses the ANI of the primary extension.

Call Vectoring

The ANI of the originating party is used, not the ANI of the call vector, when a call vectoring route-to command routes a call over an outgoing trunk.

Distributed Communications System (DCS)

In a DCS, the ANI that is sent to the CO is determined by the **ANI for PBX** field, but the category sent to the CO is determined by the **Category for MF ANI** field on the Class of Restriction screen for the incoming DCS trunk or by the type of call.

Expert Agent Selection (EAS)

The EAS agent's login extension and COR is used to determine the ANI prefix.

Hunt Groups and Automatic Call Distribution (ACD) Splits

The phone's extension and the COR is used to determine the ANI prefix for a hunt group or ACD split.

Multimedia Call Handling (MMCH)

For call origination, multimedia complexes use the COR assigned to their phones.

Remote Access

A remote access barrier code COR is not used for ANI. The extension's ANI is used if an extension originates the call. The ANI for the server is used if the originating endpoint is an incoming trunk.

Separation of Bearer and Signaling

The Separation of Bearer and Signaling feature can provide ANI while the media stream is going over a type of trunk that cannot provide ANI.

Chapter 45: Automatic Wakeup

Using Automatic Wakeup, attendants, front desk users, and guests can request an automatic wakeup call at a later time.

If the **Dual Wakeup** field on the Hospitality screen is y, then each extension can be given two wakeup call requests within 24 hours. If the **Room Activated Wakeup with Tones** field is y, wakeup calls can be activated through tones that prompt users for the time they want to be called.

Detailed description of Automatic Wakeup

Wakeup requests may be placed from 5 minutes to 23 hours and 55 minutes in advance of a wakeup call.

Depending on how automatic wakeup is administered, when a user answers a wakeup call, the system can provide:

- a recorded announcement
- a speech-synthesis announcement
- music
- silence

All wakeup times entered into the system round to the nearest five minutes. For example, a requested time of 6:58 am stores in the system as 7:00 am. The server running Communication Manager bases its time-validity checks on the rounded figure.

Wakeup calls are placed within two and one-half minutes of the requested time, and never reroute, forward, or go to coverage. Before placing the wakeup call, the system overrides Do Not Disturb for the extension.

If a wakeup-call attempt is unanswered or if the extension is busy, the system tries two more times at 5-minute intervals. If the call does not complete after 3 attempts, Communication Manager leaves an LWC message for a designated extension (usually assigned to a button on the attendant console or backup phone). The system maintains a complete record of all wakeup-call activity for the past 24 hours.

Users with touch-tone dialing can enter a wakeup request (if Wakeup Activation through Tone is enabled) or can have the front desk set a wakeup time. Users with rotary-dial phones call the front desk to request a wakeup call.

Activate Automatic Wakeup either by dialing the FAC or by pressing the automatic wakeup entry button. If the user has a display set, the system provides display prompting.

- Voice Prompting with Room Activated with Tones On

  A guest enters their wakeup-call request. The request is entered only for the extension where the call originates.

  After the user dials the Automatic Wakeup FAC, the system generates recall dial tone. This dial tone prompts the user to enter the time in a 24-hour, 4-digit format. Confirmation tone means that the wakeup request is successful.

- Display Prompting with Dual Wakeup Off

  Display prompting is provided to attendants, front-desk users, and other users with display-equipped phones. Administer front-desk users (or any other phones you want to grant permissions to) with a console permission COS to perform the same actions as the attendant. Other users can enter a wakeup request only for the extension where the call originates.

  The attendant presses the automatic wakeup entry button to activate the feature. If the attendant is on an active call with a system user, the user's extension displays as the default extension after pressing the pound sign (#). If the displayed extension is not the extension of the user requesting the wakeup call, the attendant can change it. Display prompting continues until the attendant enters all necessary information and the request for the wakeup call is confirmed.

  If a condition exists by which the system cannot accept the wakeup request, the system displays the reason for denial. Wakeup requests are denied for one of the following reasons:

  - Too Soon — Indicates that the requested wakeup time is within the current five-minute wakeup interval
  - System Full — Indicates that the maximum number of wakeup calls is reached
  - Interval Full — Indicates that the maximum number of wakeup calls in any 15-minute interval is reached

  The attendant can change or cancel a wakeup call request at any time.

- Display Prompting with Dual Wakeup On

  Display prompting with Dual Wakeup works the same as Display Prompting with Dual Wakeup off (described in the previous text), except that after the first wakeup request is entered, the user is prompted for the second wakeup request.

When the system places a wakeup call, one of the following occurs:

- Extension Is Busy — The wakeup call is placed again later.
- No Answer — The extension rings for 30 seconds. If the call is unanswered, the system tries again later.
- Ringing Blockage — If four or more ports on the same analog media module are already ringing, the system waits 16 seconds and tries again. If the second attempt is blocked, the call has failed and the system waits 5 minutes before trying again.

- Call Is Answered — The guest answers the wakeup call and hears either music, a recorded announcement, the speech-synthesizer announcement, or nothing.
- System Reset — indicates that a system reset level 1 or system reset level 2 occurred while the system attempted to place the wakeup call. Calls affected by these conditions are treated as other wakeup attempts.

If a wakeup call is incomplete because of a busy, no answer, ringing blockage, or system reset, the system attempts to place the call 2 more times at 5-minute intervals. If the call is not completed after 3 attempts, the system leaves an LWC message to account for the failed attempt.

A special extension, called the Extension to Receive Failed Wakeup LWC Messages, is administered exclusively for receiving failed wakeup-call LWC messages. When a failed message is retrieved, the display shows the date, time, and extension for the failed wakeup-call attempt.

Assign an automatic-message waiting (AMW) button and associated lamp to attendant consoles or front-desk terminals. The number associated with the button can be the wakeup-messages extension. The AMW lamp lights when a failed wakeup message is waiting. The user retrieves the message by invoking coverage-message retrieval on the wakeup-message extension. The user presses the AMW button to place the console or phone in coverage-retrieval mode. The user then retrieves the failed wakeup-call attempt messages. Only attendants and specified phone users can retrieve and delete failed wakeup messages.

The system maintains an audit-trail record of wakeup-call activity for the past 24 hours. The wakeup-call buffer can only hold a number of records equal to the maximum number of stations administrable on Communication Manager. For example, if a maximum of 200 stations is administrable, only 200 automatic-wakeup records are stored.

You can display wakeup events at the management terminal, or print to a designated printer. If the system has a journal printer, wakeup events print as they occur.

The audit trail record contains the following information:

- Type of events:
  - Request — A new wakeup-call request is made.
  - Change — The time is changed on an existing wakeup-call request.
  - Cancel — A wakeup request is canceled.
  - Move To — The wakeup request for this room moves to another room.
  - Move From — The wakeup request for another room moves from the old room to the new room.
  - Move-Cancel — A wakeup request from another room replaces the request for this room.
  - Swap — A room swap occurs and at least one of the rooms has a wakeup request. Wakeup calls swap when a room swap is performed. A journal entry is made for each room. If the room receives a wakeup call as the result of the swap, the time of the call is provided in the entry. If the room loses a wakeup call as the result of the swap (and has not received another), the time is not present in the entry.
  - Completed — The wakeup call completes successfully.

  - Not Completed — The wakeup call failed.
  - Skip — The wakeup call is skipped. This event occurs if the system time advances past the requested time of a wakeup call.
- Time of the event
- Extension number receiving the call
- Time of the wakeup request
- Extension (or 0 for the attendant) where the event took place
- Number of call attempts that were placed
- An indication of why a wakeup-call attempt failed

In addition, all wakeup-time changes are recorded. This record shows the original time requested and the changed time. The audit-trail record is not backed up and all wakeup data is lost if a system failure occurs.

Schedule the following reports for printing on a daily basis:

- Wakeup Activity report – summarizes wakeup activity for each extension that had any wakeup activity over the past 24 hours.
- Wakeup Summary report —gives an hour-by-hour summary of the number of scheduled wakeup calls, the number of wakeup calls completed, and a list of extensions. The report covers all automatic-wakeup events for each hour over a 24-hour period.

With VDNs and multiple announcements, you can choose as the announcement extension a VDN that reaches one announcement if the system clock is less than 12:00 and another if the system clock is greater than 12:00. The hotel guest hears “good morning” before noon and “good evening” after noon. Or, a business customer can choose as the announcement extension a VDN that points to an extension assigned to a quorum bridge, with the wakeup time as a scheduled teleconference time. When the wakeup call is completed, the customer automatically connects to the teleconference bridge.

You can administer a multiple announcement to repeat. To enable repeating announcements, enter announcement type integ-rep command on the Recorded Announcement screen. With repeating integrated-message functionality, the announcement keeps repeating from when the first guest (of a group of guests receiving the same wakeup announcement simultaneously) goes off-hook until the last guest goes on-hook.

If the announcement type is either an externally-recorded announcement or is integrated-repeating, you can administer the wakeup-call queue for barge-in. Barge-in means that the guest receiving the wakeup call hears the announcement as soon as they are off-hook, even if the announcement is not at the beginning. This provides the capability of many users being bridged onto the same announcement port, eliminating the need for a separate port for each wakeup call. See Recording Announcements for additional information.

Considerations for Automatic Wakeup

This section provides information about how the Automatic Wakeup feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Automatic Wakeup under all conditions. The following considerations apply to Automatic Wakeup:

- Up to 10 attendant consoles and/or front desk terminals may be in the wakeup display mode at any one time.
- More than one alphanumeric name can refer to the same digit string.

Interactions for Automatic Wakeup

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

Attendant or Phone Display

If the console or phone is in automatic-wakeup mode and the user presses another display-mode button, wakeup mode aborts and the wakeup request is not entered, changed, or deleted.

Do Not Disturb

If Do Not Disturb is active at a phone, Automatic Wakeup deactivates Do Not Disturb for that terminal, and the system places the wakeup call.

PMS Interface

A Check-Out request cancels an active-wakeup call request for the guest room. Room Change/ Room Swap requests through PMS cause a wakeup request to change or swap.

Chapter 46: Avaya Video Conferencing Solution

Avaya Video Telephony Solution provides videoconferencing abilities for your desktop and group video communications. Avaya Video Conferencing Solution can be administered in the following ways:

Avaya Aura® Conferencing without external gatekeepers or MCUs

This configuration does not involve external MCUs or external gatekeepers. All endpoints are H.323-based and registered to Communication Manager or SIP-based and registered to Session Manager. Scopia XT5000 includes an optional embedded MCU.

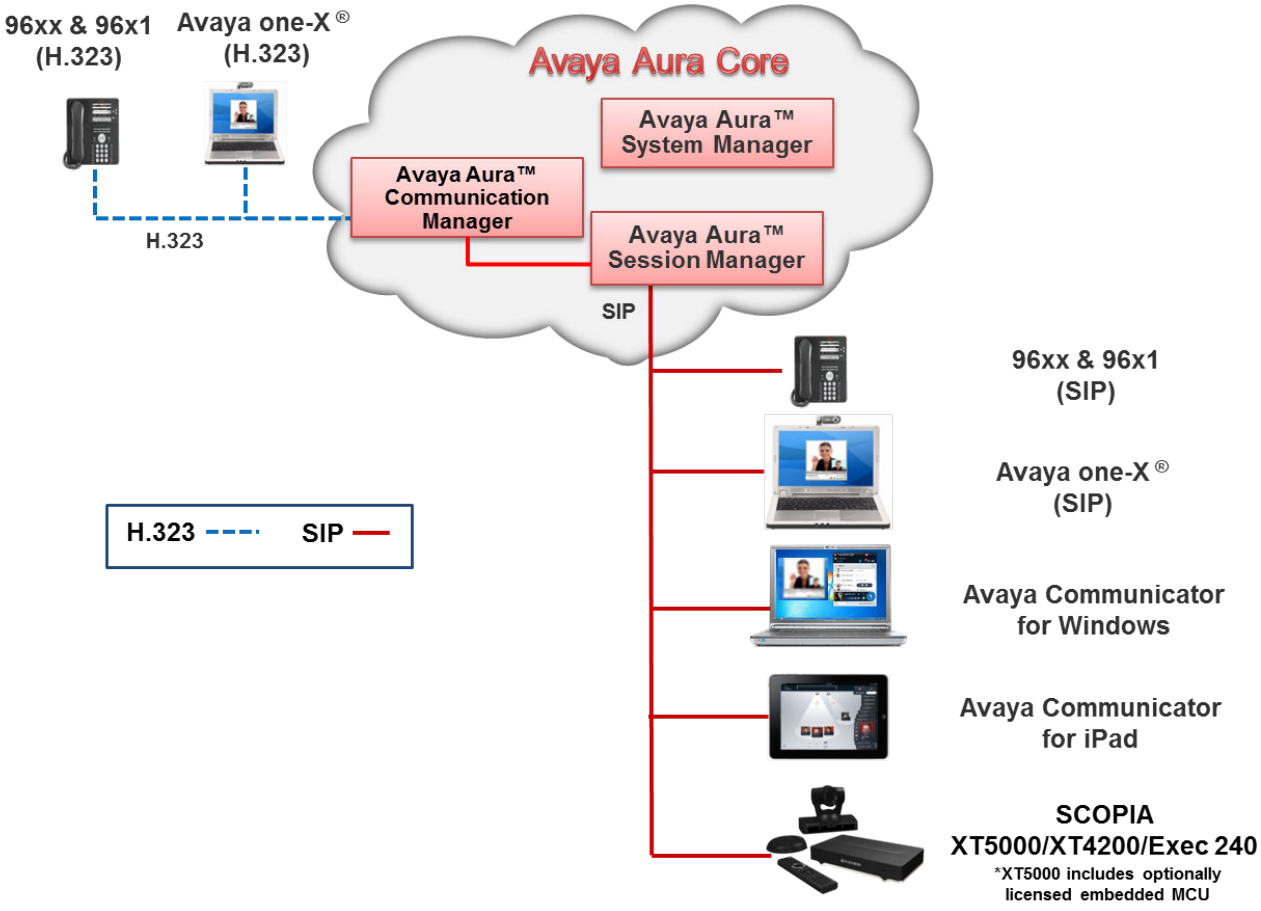


Figure 3: Avaya Aura® Conferencing without external gatekeepers or MCUs configuration

Avaya Aura® and Scopia interoperability

An H.323 trunk between Communication Manager and Scopia ECS Gatekeeper. Point-to-point calls between H.323-based and SIP-based Avaya video endpoints and H.323-based Scopia endpoints connect through the H.323 trunk. Conference calls that are hosted on the Scopia Elite MCU and involve H.323-based Avaya video endpoints connect through the H.323 trunk.

A SIP trunk between Session Manager and the B2BUA component of Scopia iView Management Suite Release 7.7 or Scopia Management Release 8.3.

Conference calls that are hosted on Scopia Elite MCU and involve SIP-based Avaya video endpoints connect through the SIP trunk.

Note:

Avaya audio endpoints can connect to Scopia Elite MCU through the H.323 trunk or through the SIP trunk.

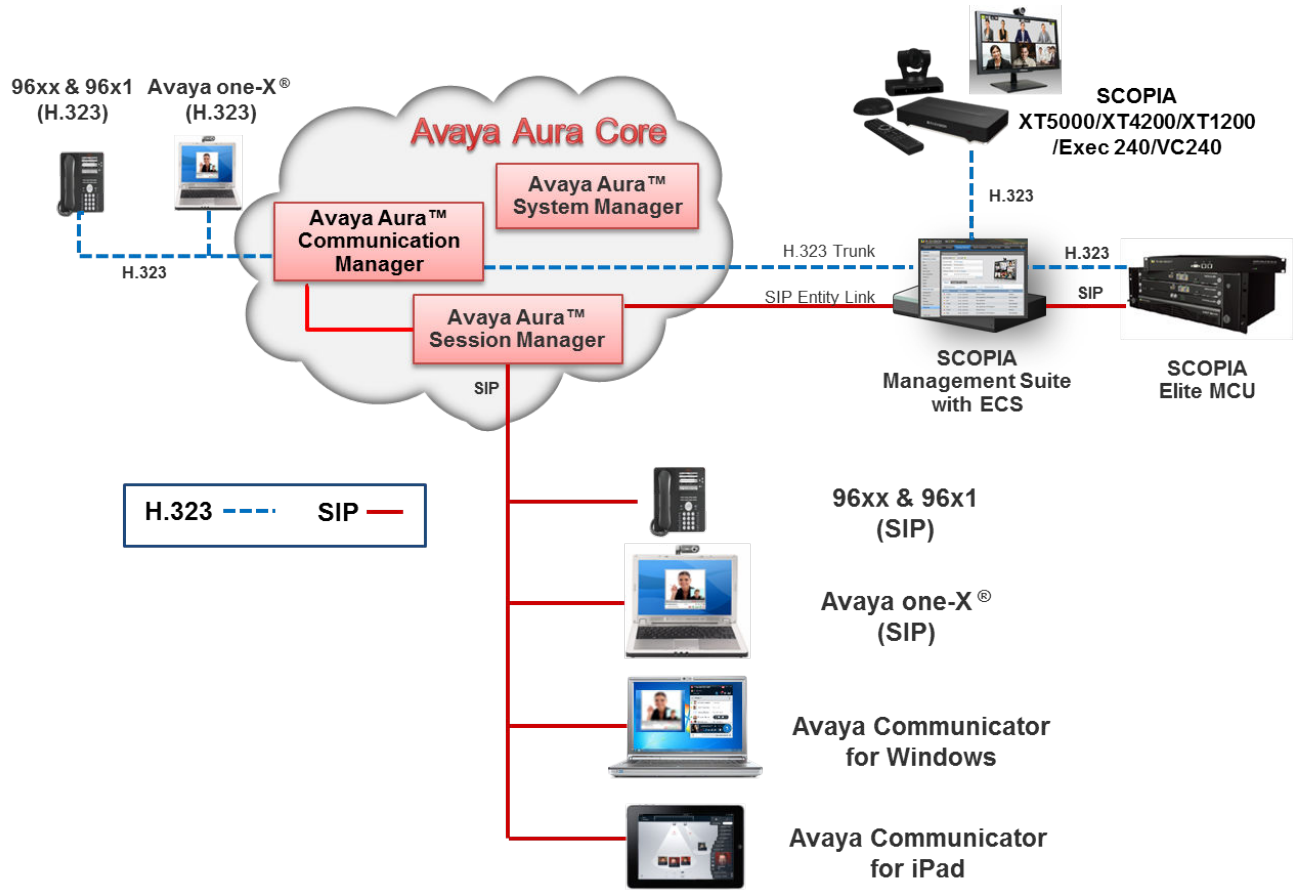


Figure 4: Avaya Aura® and Scopia interoperability

Avaya Aura® and Scopia interoperability with third-party endpoints

This configuration involves third-party endpoints that register to Scopia ECS Gatekeeper in the interoperability between Avaya Aura® and Scopia.

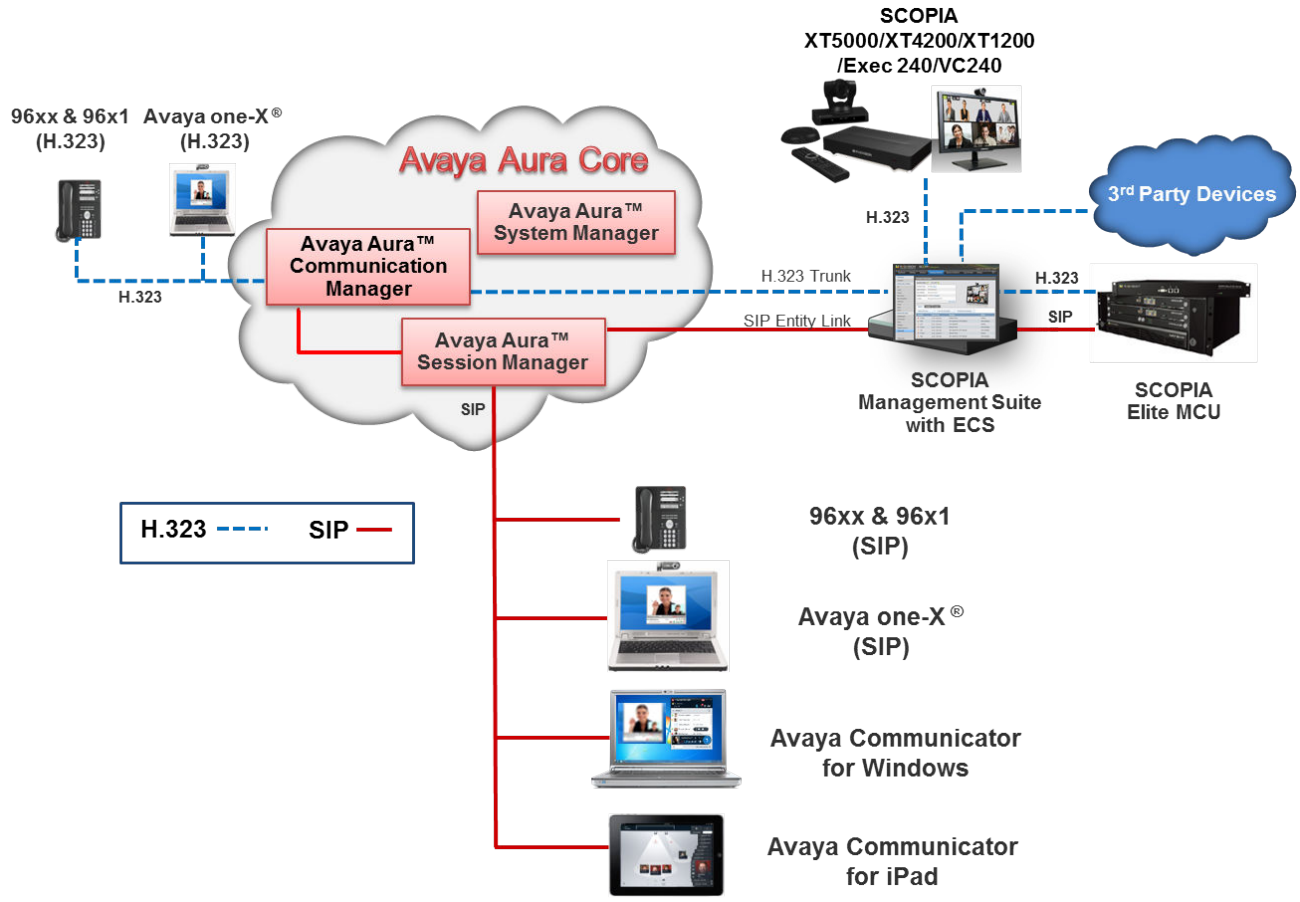


Figure 5: Avaya Aura® and Scopia interoperability with third-party endpoints

Note:

Point-to-point video calls between Avaya Aura® video endpoints and third-party endpoints connected to Scopia Management are not supported. These calls must connected through the Elite MCU.

Avaya Aura® with the external Polycom MCU and H.323-based endpoints

In this configuration, Polycom is integrated directly into Avaya Video Conferencing Solution. Polycom HDX series endpoints are registered directly to Communication Manager. The Polycom RMX MCU is administered for dual connectivity as:

- An H.323 trunk to Communication Manager
- A SIP trunk to Session Manager

An H.323 trunk to Communication Manager. A SIP trunk to Session Manager.

Call routing is administered to ensure that call routes are established between these two trunks based on the protocol of the endpoint. For example, a SIP-based call route is established through the SIP trunk between Polycom RMX and Session Manager, while an H.323-based call route is established through the H.323 trunk between Polycom RMX and Communication Manager.

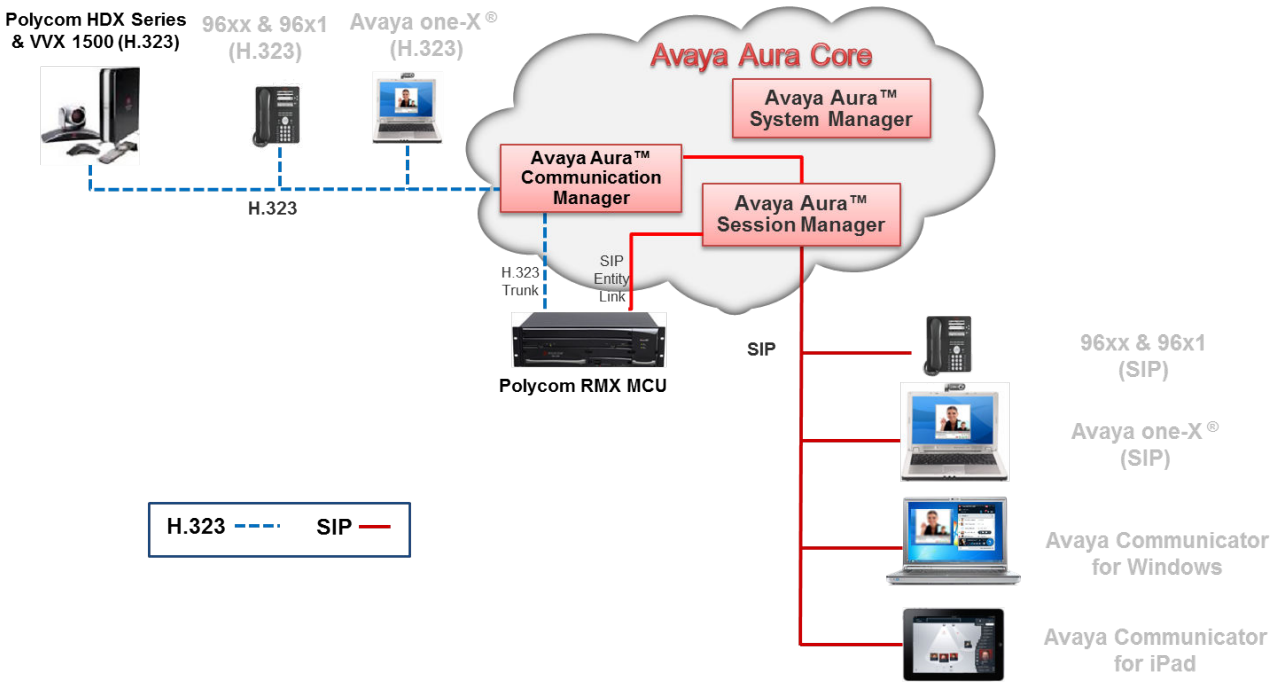


Figure 6: Avaya Aura® with H.323-based Polycom endpoints through Communication Manager and Polycom RMX.

Avaya Aura® with the external Polycom MCU and SIP-based endpoints

This configuration involves the external Polycom MCU and SIP-based endpoints in the direct integration of Polycom with Avaya Video Conferencing Solution. Polycom HDX series and Polycom VVX 1500 endpoints are SIP-based in this interoperability solution.

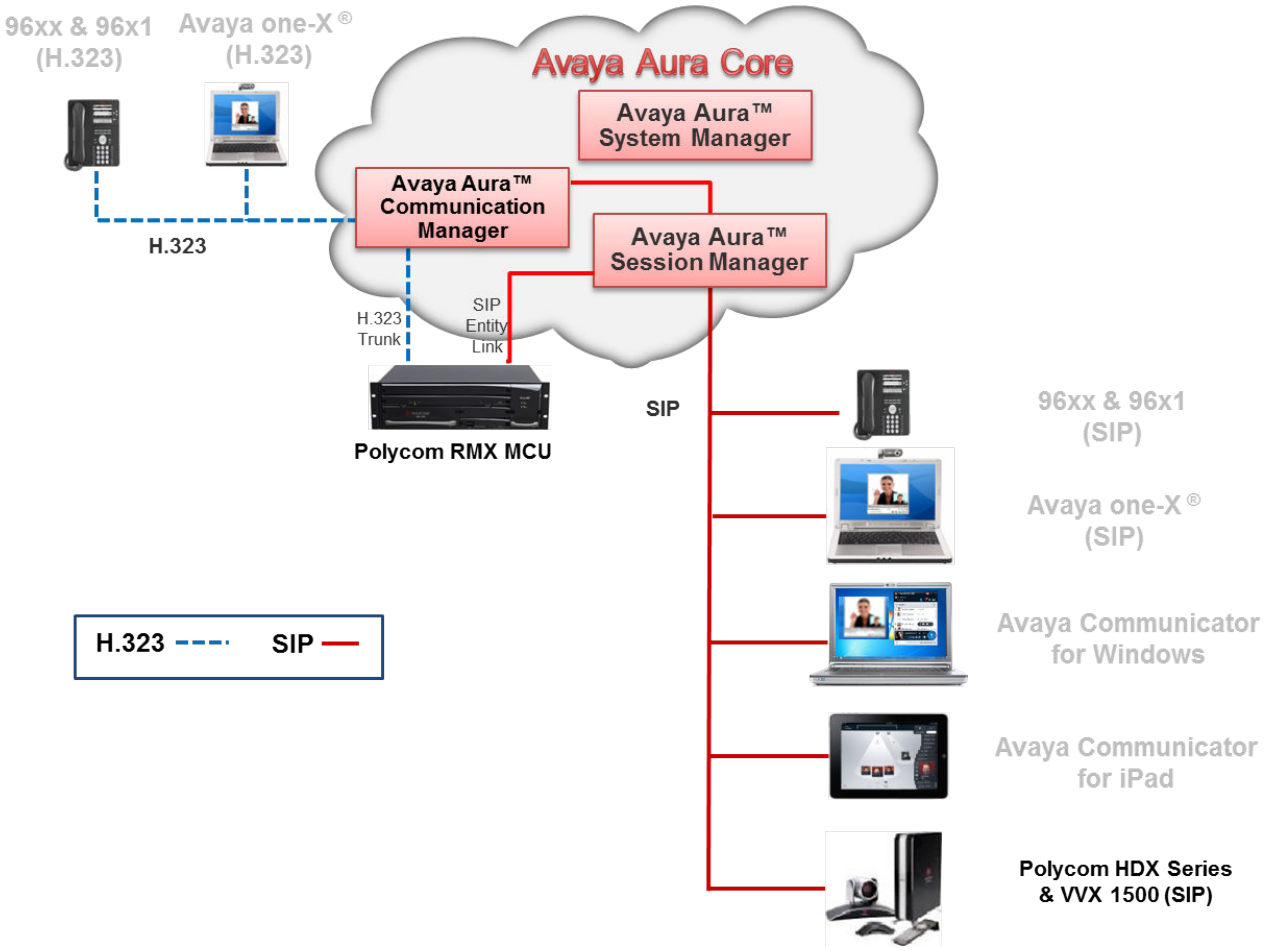


Figure 7: Avaya Aura® and SIP-based Polycom endpoints interoperability

Avaya Aura® and Polycom interoperability

Avaya Aura® is integrated with and Polycom through:

- Polycom RMX MCU administered for dual connectivity: An H.323 trunk to Communication Manager and a SIP trunk to Session Manager.
- Polycom DMA Gatekeeper or Polycom CMA Gatekeeper: An H.323 trunk to Communication Manager. Point-to-point calls between H.323-based and SIP-based Avaya video endpoints and H.323-based

Point-to-point calls between H.323-based and SIP-based Avaya video endpoints and H.323-based Polycom endpoints connect through the H.323 trunk. Conference calls that are hosted on the Polycom RMX MCU and involve H.323-based Avaya video endpoints connect through the H.323 trunk.

Call routing is administered to ensure that call routes are established between these two trunks based on the protocol of the endpoint. For example, a SIP-based call route is established through the SIP trunk between Polycom RMX and Session Manager, while an H.323-based call route is established through the H.323 trunk between Polycom RMX and Communication Manager.

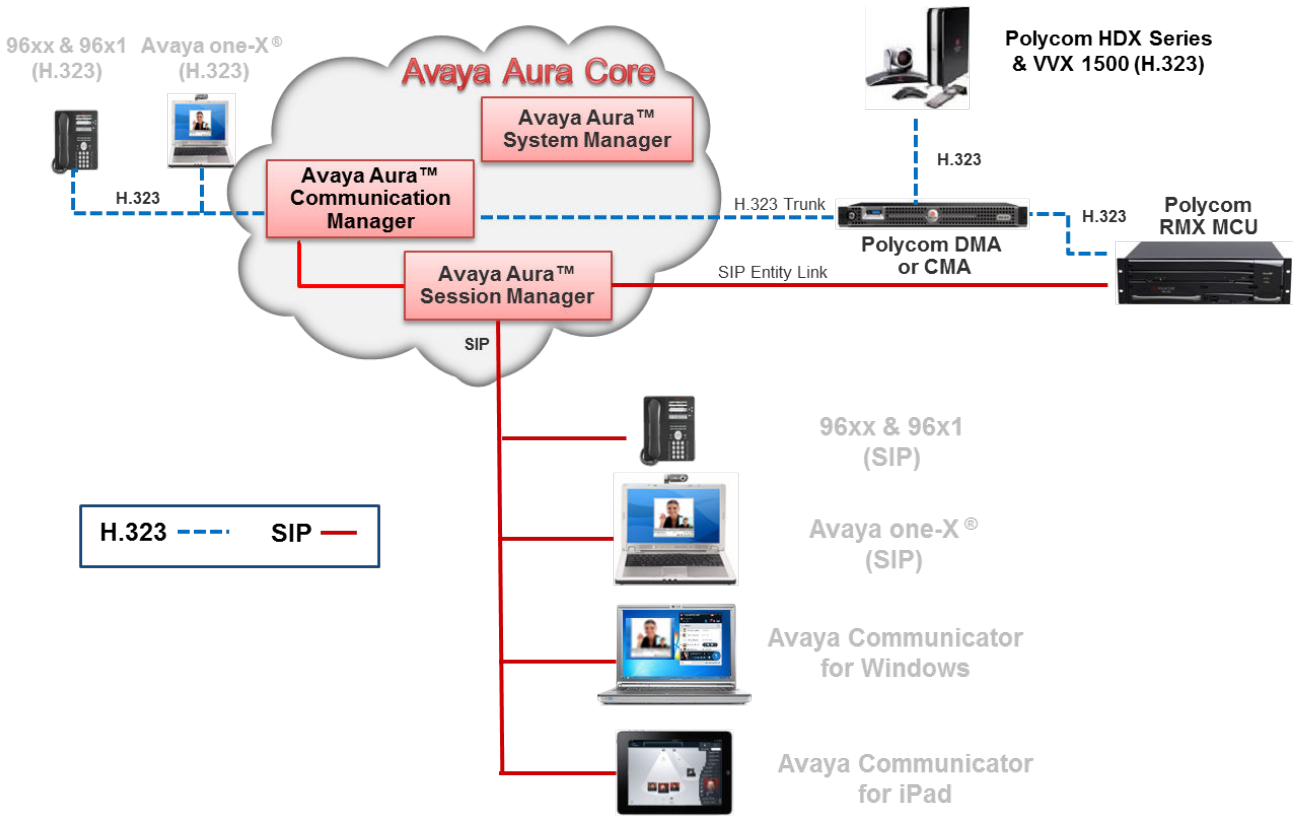


Figure 8: Avaya Aura® and Polycom interoperability

For more information, see *Administering Avaya Video Conferencing Solution Quick Setup*.

Video SRTP and TLS support with Scopia 8.3

TLS and SRTP encryption is supported between Session Manager and Scopia® solution products, providing higher security within mixed Scopia® solution and Avaya Aura® environments. This support is available with the upcoming Scopia 8.3 service pack.

The MCU, a device used to bridge videoconferencing connections, can encrypt communications with endpoints to create secure connections with H.235-based encryption for H.323 endpoints and SRTP and TLS encryption for SIP endpoints.

Communication Manager supports SRTP for video call flows only when the call originating and the receiving endpoints are SIP-registered and the IP-codec-set administration on Communication Manager is SRTP. H.323-registered endpoints always send video RTP. SIP-H.323 interworking with video encryption is not supported and video is blocked in this case. However, if the **Best effort SRTP** mode is selected,Communication Manager allows video RTP to pass through.

For more information about administering SRTP for video signaling, see *Administering Network Connectivity on Avaya Aura® Communication Manager*.

Chapter 47: Bridged Call Appearance

Use the Bridged Call Appearance feature to give single-line and multiappearance telephones an appearance of another telephone number. With Bridged Call Appearance, the user can originate, answer, and bridge onto calls to or from the telephone number of another user.

The terms “primary number,” “primary telephone,” and “primary station” all mean the same thing. The primary number is the extension that you want other extensions to bridge onto. For example, if you want extension A as the primary number to also have call appearances on extensions B, C, and D, the administrator must access extensions B, C, and D using the Station screen, and bridge each extension to extension A.

The Bridged Call Appearance feature works on the following telephones:

Single-line telephone

A single-line telephone can be the primary number, meaning that it can have a bridged appearance on another telephone. A single-line telephone can also have a bridged appearance of either another single-line telephone or a multiappearance telephone.

Multiappearance telephone

A multiappearance telephone can be the primary number, meaning that it can have a bridged appearance on another telephone. A multiappearance telephone can have a bridged appearance of a single-line telephone or one or more appearances of a multiappearance telephone. A multiappearance telephone can also have bridged appearances of multiple telephone numbers.

Detailed description of Bridged Call Appearance

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.

If a call is transferred from a bridged appearance to another number and the call goes unanswered, the call returns to the bridged appearance. The call does not return to the primary number. On a bridged station without a line appearance, the call originator hears a reorder tone after the transfer recall timer expires.

For example, a user calls the primary number B and the call is answered from station A, the bridged appearance of station B. Station A performs a blind transfer to another station D, but the call is unanswered. The unanswered call returns to the call appearance of station A.

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. To avail this feature, set the **Match BCA Display to Principal** field on page 2 of the COS screen 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.

Administrable buttons and lamps for multiappearance telephones

You can administer the message lamp and some feature buttons to apply to the primary number rather than to the number of the telephone they reside on.

- You can administer the message lamp to light on the bridged user's telephone when messages are waiting for the primary telephone.
- You can administer the call forwarding all calls and call forwarding busy/don't answer buttons to activate Call Forwarding for any extension that is on the telephone, even if this extension is a bridged appearance. In addition, you can administer the lamp associated with the call forwarding button to track the call forwarding status of any extension. Thus, a bridged user can activate or deactivate Call Forwarding from the telephone with the bridged

call appearance for all primary and bridged appearances of the extension. The bridged appearance telephone shows the call forwarding status of the specified extension.

- You can administer the send all calls button to activate Send All Calls for any administered extension. The lamp associated with Send All Calls tracks the status of the administered extension. Thus, a bridged user can activate Send All Calls for the primary extension user.

Bridged Call Appearance administration

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

- Creating a bridged call appearance on a single-line telephone
- Creating a bridged call appearance on a multiappearance telephone

Related links

Creating a bridged call appearance on a single-line telephone on page 314
Creating a bridged call appearance on a multiappearance telephone on page 315

Preparing to administer Bridged Call Appearance

Procedure

1. If Data Privacy for data or voice calls is administered, you can prohibit bridging onto voice or data calls with Data Privacy.

   To prohibit bridging onto Data Privacy calls, type `y` in the **Prohibit Bridging Onto Calls with Data Privacy** field on the Feature-Related System Parameters screen.

   To view the Feature-Related System Parameters screen, type `display system-parameters features`. Press `Enter`.

2. For each coverage path that includes a telephone with bridged appearances you must administer whether you want a call to skip a coverage point if that telephone has already alerted as a bridged appearance.

   Enter `n` to skip the coverage point in the **Terminate to Coverage Pts. with Bridged Appearance?** field on the Coverage Path screen. Enter `y` to alert both a bridged call and a redirected call.

   To view the Coverage Path screen, type `change coverage path` *n*, where *n* is the number of the coverage path you want to change. Press `Enter`.

Screens for administering Bridged Call Appearance

Screen name	Purpose	Fields
Feature-Related System Parameters	Ensure data privacy.	Prohibit Bridging Onto Calls with Data Privacy
Coverage Path	Skip a coverage point.	Terminate to Coverage Pts. with Bridged Appearance
Station	Create a bridged call appearance on a single-line telephone	• Bridged Call Alerting • Line Appearance • Btn • Ext
	Create a bridged call appearance on a multiappearance telephone	• Per Button Ring Control • Bridged Call Alerting • Bridged Idle Line Appearance • Auto Select Any Idle Appearance • Button Assignments • Btn • Ext • Ring

Creating a bridged call appearance on a single-line telephone

Procedure

1. Type `change station n`, where *n* is the extension of the single-line (analog) telephone on which you want to create the bridged call appearance. Press `Enter`.
2. On the Station screen, click `Next` until you see the **Bridged Call Alerting?** field.
3. In the **Bridged Call Alerting?** field, perform one of the following actions:
   - If you want the bridged appearance to ring when a call arrives at the primary telephone, type `y`.
   - If you want the bridged appearance to flash but not ring when a call arrives at the primary telephone, leave the default set to `n`.
4. Click `Next` until you see the **Line Appearance** field.
5. In the **Line Appearance** field, perform one of the following actions:
   - Type `abrdg-appr` to create a bridged appearance of a single-line telephone.
   - Type `brdg-appr` to create a bridged appearance of a multiappearance telephone.
6. Press `Enter`.

   The system displays the **Btn** and **Ext** fields.

7. In the **Btn** field, type the button number from the primary telephone that you want to use for the bridged call appearance.
8. In the **Ext** field, type the extension of the primary telephone.
9. Press `Enter` to save your changes.

Creating a bridged call appearance on a multiappearance telephone

Procedure

1. Type `change station` *n*, where *n* is the extension of the multiappearance telephone on which you want to create the bridged call appearance. Press `Enter`.
2. On the Station screen, click `Next` until you see the **Per Button Ring Control?** field.
3. Perform one of the following actions:
   - Type `y` to assign ringing separately to each bridged appearance.
   - Leave the default setting, `n`, to assign all bridged appearances to either ring or not ring as determined by the **Bridged Call Alerting** field.
4. In the **Bridged Call Alerting?** field, perform one of the following actions:
   - Type `y` if you want the bridged appearance to ring when a call arrives at the primary telephone.
   - Leave the default setting, `n`, if you want the bridged appearance to flash but not ring when a call arrives at the primary telephone.
5. In the **Bridged Idle Line Preference?** field, perform one of the following actions:
   - Type `y` if you want the user to lift the telephone receiver, then press the lighted bridged appearance button to connect to the call.
   - Leave the default setting, `n`, if you want the user to just lift the telephone receiver to connect to the call
6. In the **Auto Select Any Idle Appearance?** field, perform one of the following actions:
   - Type `y` to allow automatic selection of an alternate idle appearance for transferred or conferenced calls when another appearance of the bridged number is unavailable.
   - Leave the default setting, `n`, to prevent this automatic selection.
7. Click `Next` until you see the **Button Assignments** area.
8. In the **Button Assignments** area next to any available button number, perform the following actions:
   - Type `abrdg-appr` to create a bridged appearance of a single-line telephone.
   - Type `brdg-appr` to create a bridged appearance of a multiappearance telephone.
9. Press `Enter`.

The system displays the **Btn** and **Ext** fields.

10. In the **Btn** field, enter the button number from the primary phone that you want to use for the bridged call appearance.
11. Enter the extension of the primary telephone.
12. Press `Enter` to save your changes.

Considerations for Bridged Call Appearance

This section provides information about how the Bridged Call Appearance feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Bridged Call Appearance feature under all conditions.

The following considerations apply to single-line telephones:

- A bridging user cannot have more than one bridged appearance for a particular primary telephone. However, a multiappearance bridging user can have bridged appearances of more than one single-line telephone on their telephone (a multiappearance bridging user, by use of different buttons, can bridge onto several different primary telephones).
- If the primary single-line telephone is correctly administered, but not in service, calls can still be placed by the bridging users, and received on the bridged appearances of the telephone.
- If more than one user goes off-hook on a bridged appearance at the same time, only the user who was the first to go off-hook can dial.
- The Privacy-Manual Exclusion feature can be activated by the bridging user only, while active on a call, to prevent accidental bridging of an active call.
- If a call terminates at a telephone on an extension other than the primary extension (for example, terminating extension group (TEG), UCD group, call coverage answer group, or DDC group extension), a bridged call appearance is not maintained. Therefore, the primary telephone should not be made a member of such a group.
- If two parties are bridged together on an active call with a third party, and if the conference tone feature is enabled, conference tone is heard.
- When a station A has brdg-appr button of the station B, and a call is made from station B to station C. If this call is answered on station C, the name and number of station C does not appear on the brdg-appr button on station A in order to honor the privacy of station B.

The following considerations apply to multiappearance telephones:

- On multiappearance telephones, a bridged call appearance can be assigned to any 2-lamp button. It does not require the use of a regular call appearance. The number of bridged call appearances allowed at each telephone is limited only by the number of 2-lamp buttons available on the telephone.

- Up to six parties can be off-hook and involved in a conversation on a bridged appearance of an extension. However, if the **12–party Conferences** field is enabled in the Feature-Related System Parameters screen, 12 parties can participate in a conference call.
- A bridging telephone might have a bridged call appearance corresponding to each call appearance of the primary extension at the bridged telephone. For example, if a primary telephone has three call appearances, a bridging telephone should have three bridged call appearances of that primary extension. Using this feature, users can refer to the individual call appearances when talking about a specific call.
- Bridged call appearances may result in the reduction of available feature buttons, thereby reducing a user's capabilities. You can use a Call Coverage module or expansion module to provide additional bridged call appearances.
- If a call terminates at a telephone on an extension other than the primary extension, a bridged call appearance is not maintained. Examples of such termination points can be TEG, UCD group, call coverage answer group, or DDC group extensions. Therefore, the primary telephone should not be made a member of such a group.
- You can administer conference tone, which, when enabled, is heard when two parties are bridged together on an active call with a third party.
- You can administer a telephone with zero call appearances of its primary extension. In this way, a telephone can be administered to have only bridged appearances.

Interactions for Bridged Call Appearance

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

Abbreviated Dialing

A user, accessing Abbreviated Dialing while on a bridged call appearance, accesses their own Abbreviated Dialing lists. The user does not access the Abbreviated Dialing lists of the primary extension associated with the bridged call appearance.

A user cannot use an abbreviated dialing Feature Access Code (FAC) after using a priority calling FAC.

Adjunct Switch Applications Interface (ASAI)

If you are using ASAI, do not administer more than 16 bridged appearances. When Communication Manager enables ASAI, it allows call recording application to record bridged line appearances.

Attendant display and telephone display

A call from the primary extension or from a bridged call appearance of the primary extension is displayed as a call from the primary extension. That is, the call is displayed as coming from the primary extension regardless of which appearance placed the call.

On multiappearance telephones, the display at the primary telephone shows the same information for a bridged call appearance as the information for a nonbridged call. For calls to the primary

extension, the display at a zero call appearance bridging telephone shows a call from the originator to the primary with no “redirection reason” character.

Automatic Call Distribution (ACD)

Bridged appearances cannot be accessed using non-ACD hunt groups (although administrable).

Automatic Callback

Automatic Callback calls cannot originate from a bridged call appearance. However, when Automatic Callback is activated from the primary telephone. The callback call rings at all bridged appearances of the extension and at the primary telephone. This ring is set with priority call distinctive ringing signal. It displays at all telephones and shows that it is a callback call.

Busy Indicator (multiappearance telephones only)

A user presses a **Busy Indicator** button to call the extension associated with the **Busy Indicator** button. When a user presses a **Busy Indicator** button on a zero primary call appearance telephone, the system uses the first available bridged call appearance to place the call.

Call Coverage

Single-line telephones:

When a single-line telephone is administered as a bridged call appearance, the telephone user cannot invoke Send All Calls for the extension of their telephone. The user does not have a send all calls button, and the call appearance is associated with another extension. When the user dials a FAC, Send All Calls is activated for the extension associated with the call appearance.

Multiappearance telephones:

Coverage criteria for bridged call appearances is based entirely on the criteria of the primary extension associated with bridged appearance. A call to the primary extension that requires call coverage treatment follows the coverage path of the primary extension. Such a call does not follow the path of any of the bridged appearances. Bridged call appearances do not receive redirection notification.

A user with bridged call appearances can activate or deactivate Send All Calls for a primary telephone from the bridged appearance.

The primary telephone should not be a member of a call coverage group. This is because calls to the primary telephone as a member of the group are not bridged.

You can administer the system so that a telephone displays both a bridged call and a redirected call. In this way, if the bridged user is the first coverage point, the call redirects to that telephone when the coverage criteria are satisfied.

If the primary telephone is a single-line telephone with a bridged call appearance on a multiappearance telephone, an incoming call to the single-line telephone that goes to coverage terminates at a primary call appearance on the bridging user’s telephone as a coverage call. If the bridging user is a zero primary call appearance telephone, the call cannot redirect to the bridging user. This is because there are no primary call appearances. Therefore, the call redirects to the next available coverage point.

Call Detail Recording (CDR)

If a bridging user originates or answers a call on a bridged appearance, the extension of the bridge is recorded as the calling/called telephone. A conference or transfer by a bridging user also seems as it was performed by the telephone user.

On multiappearance telephones, when a call originated from a bridged call appearance on a telephone administered for zero primary call appearance is recorded by CDR, the extension associated with the appearance is recorded as the calling party. A conference or transfer by a bridged call appearance on a zero primary call appearances telephone also appears as performed by the extension associated with the appearance.

Call Forwarding All Calls, Call Forward Busy/Don't Answer

Call Forwarding can be activated or canceled for the primary extension from any bridged call appearance of that number. When activated, calls to the primary extension do not terminate at the bridged call appearances, but go to the designated forwarding destination. Bridged call appearances do not receive redirection notification of the call to the primary extension when it is forwarded unless Ringing - Abbreviated and Delayed is administered.

Call Park

When a call is parked from a bridged call appearance, it is parked on the primary extension.

Call Pickup

Calls that are made to a primary telephone, alerting at bridged appearances of the primary telephone, can only be answered by pickup group members of the primary number.

- If the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to `n`, the primary appearance and all bridged appearances of the call are dropped after Call Pickup is used to answer the call.
- If the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to `y`, the primary and bridged call appearance lamps stay lit after Call Pickup is used to answer the call.
- If the primary telephone and the bridged telephone are both in the same pickup group, members in the pickup group can answer a call that is made to the primary telephone that is ringing at the bridging user's telephone. This can be done instead of selecting the bridged appearance button.
- If the primary telephone and the bridged call appearance are not in the same pickup group, members who are in the same pickup group as the bridged call appearance telephone can answer a call that is made to the primary telephone.

When a user dials the Call Pickup FAC on a bridged call appearance, the system interprets the action as an attempt to answer a call from the call pickup group of the primary telephone. When operating this way, the covering user can act as the primary user and provide the same call pickup coverage if required.

If a telephone has bridged call appearances of numerous telephones, for example, sales, service, and warehouse, and you want calls to be answered only by the primary telephone users or the bridging users, do not assign the primary and bridging users to a pickup group.

Call Waiting Termination (single-line telephones only)

Call Waiting Termination applies only to an active call on the primary telephone that has no one else bridged on. If one or more bridging users are active on a call, waiting calls are denied even if the primary user is also off-hook on the call. A bridging user can bridge onto a call with the primary user if there is also a call waiting.

Class of Restriction (multiappearance telephone users only)

The COR assigned to a telephone's primary extension also applies to calls originated from a bridged call appearance.

Conference - Attendant, Conference

Single-line telephones:

A bridged call cannot be conferenced if more than one user is active on that call. This is because the bridging user has no access to the call after the primary telephone user places the call on soft hold, and the primary telephone user has no access to the bridging user's call appearance used for conference/transfer attempts.

You can place a call on hold using normal single-line conference procedures when the primary telephone user is active on a call, and no other bridging user is active on the call. Any attempt by a bridging user to bridge onto the call during a successful conference attempt is denied.

A single bridging user can conference the call using the normal multiappearance telephone conference procedures. Any attempt by the single-line primary telephone user to bridge onto the call during a successful conference attempt is ignored. Any attempt by other bridging users is denied (standard denial response is returned to the bridged appearance).

If a conference is not supported because of the preceding limitations, the user can accomplish a transfer by asking an internal nonbridged party in the connection to create the conference. The user can also ask the remaining bridging users and primary user to disconnect so that the conference can be completed. At completion of the conference, the parties that left the call can reenter the call if control of the conference remains with the primary telephone. If conference control does not remain with the primary telephone, the bridging user must conference the primary telephone and the bridging user back into the call as required.

If the bridging user has no other available bridged appearances of the primary extension (other than the one he or she is currently on), the bridging user, after pressing the conference/transfer button, must select a call appearance to be used for the conference, before dialing the number.

Multiappearance telephones:

Conferences can be set up on bridged appearances using the usual conference operations. Either a primary extension button or a bridged appearance button can be used to make the calls for adding to the conference. You can administer the system to automatically select the first idle appearance if there is no idle appearance with an extension matching the extension that is conferencing the call.

Note:

For SIP telephones, you cannot administer the system to automatically select the first idle appearance if there is no idle appearance with an extension matching the extension that is conferencing the call.

When the user presses the conference button (the second time) to connect the parties together, the system displays the newly formed conference call on the primary or bridged appearance to which the user was connected at the time of that last conference button depression. The other appearance is disassociated from the conference call. Therefore, if the original call is on a bridged appearance, and the conference is formed on a primary appearance at that same telephone, the bridged extension becomes disassociated from the conference call. In this case, the primary user can no longer bridge onto the conference.

This disassociation of the conference from the bridged extension can be avoided by setting up the conference in the opposite order. To do this, the user:

1. Presses the hold button to hold the original call on the bridged appearance
2. Selects a call appearance and calls the party to be added
3. Presses the conference or transfer button
4. Selects the held bridged appearance
5. Presses the conference button (again)

When this procedure is used, the conference is formed on the bridged appearance so that the primary user can still bridge onto the conference call.

If the primary user and the bridged user are both on the call when one user transfers the call, the user performing the transfer becomes the controlling user for the participation of both users on the conference. To disassociate the appearance from the call, the controlling user must be the latter of the two users to disconnect from the call. If the controlling user disconnects first, the appearance goes on soft hold when the noncontrolling party disconnects. In this case, one of two things must occur to disassociate the appearance from the call: all other parties on the call disconnect, or the controlling user rejoins the call and disconnects again.

The display shows the number of other active parties in a call, including active bridged appearances.

Consult (multiappearance telephones only)

Bridged call appearances of the primary extension do not ring on a consult call to the primary extension.

Coverage Answer Group

Single-line telephones:

Calls to the primary telephone as a member of a Coverage Answer Group are not bridged.

If the primary telephone is made a member of a coverage group, coverage criteria is based entirely on the criteria of the primary telephone. This means that a call to the primary telephone that requires call coverage treatment follows the path of the primary telephone and not the path of any of the telephones with bridged appearances of the primary telephones.

Multiappearance telephones:

Bridged call appearances of a primary extension do not ring when there is a Coverage Answer Group (CAG) call to the primary extension. Bridged call appearances cannot bridge onto the call.

Data Privacy, Data Restriction

When Data Privacy is activated or Data Restriction is assigned to a telephone involved in a bridged call and the primary telephone and/or bridging user attempts to bridge onto the call, Data Privacy and Data Restriction are automatically overridden (or deactivated in the case of Data Privacy).

Emergency calls

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

Note:

Avaya recommends that you administer at least one call appearance as primary call appearance. If you fail to administer at least one call appearance as primary call appearance, the public safety answering officer is unable to call back.

Hold - Automatic

Single-line telephones:

A call cannot be put on hold if more than one user is active on that call.

The primary telephone user, when no other bridges are active on the call, can put the call on hold, using normal single-line hold procedures. If the primary telephone user successfully soft holds the call, the status lamp at all of the bridged appearances shows the hold indication; and then the call can be put on hard hold by dialing the hard hold FAC. The hard held call is no longer accessible to the bridging users until it is taken off hold by the primary telephone user. After the call is put on hard hold, any new call to the primary telephone is tracked by the bridged appearances.

A bridging user can place an active call on hold (if the primary telephone or any other bridges are not active on the call) by using normal multiappearance hold procedures. Any attempt to enter the held call returns it to the status of an active call that can then be accessed using bridging procedures.

Multiappearance telephones:

Any user (primary or bridged appearance) can place an active call on hold. If only one user is active on a call and places that call on hold, the indicator lamp at both the primary's appearance button and the bridged appearance button show that the call is on hold. If more than one user is bridged onto the active call, and one of the users activates Hold, the activator receives "hold" indication for the call and status lamp of all other bridged users remains active.

Hotline Service (single-line telephones)

If a single-line telephone is administered for Hotline Service, bridged appearances of that telephone's extension also place a hot line call automatically when a user goes off-hook on that bridged appearance.

Hunt Group (DDC or UCD)

Bridged call appearances cannot be used in conjunction with DDC or UCD hunt groups.

Although you can assign a bridged extension to a hunt group, Avaya does not recommend such assignment because DDC/UCD calls do not terminate at any bridged appearances of that extension on other telephones.

Intercom (multiappearance telephones only)

Bridged appearances of a primary extension are not rung for intercom calls. Furthermore, if a telephone has no primary call appearances it can never be rung for an intercom call. Therefore, if someone is screening all calls for the primary telephone, and is indicating who is calling through intercom, the primary telephone must have a call appearance on which to receive and send intercom calls.

Internal Automatic Answer (IAA)

Calls terminating to a bridged appearance of an IAA-eligible telephone are ineligible for IAA.

Last Number Dialed (LND)

Activation of the LND feature causes the last number dialed from the activating telephone to be redialed, regardless of the extension used (primary or bridged call appearance).

Leave Word Calling (LWC)

A LWC message left by a user on a bridged call appearance leaves a message for the called party to call the primary extension assigned to the bridged call appearance.

When a user calls a primary extension, and activates LWC, the message is left for the primary extension, even if the call was answered at a bridged call appearance.

LWC messages left by the primary user can be canceled by a bridged appearance user.

Personal Central Office Line

Single-line telephones:

A single-line primary telephone cannot be a member of a Personal Central Office Line (PCOL) group.

Multiappearance telephones:

If a user is active on his or her primary extension on a PCOL call, bridged call appearances of that extension cannot be used to bridge onto the call. The call can only be bridged onto the call if another telephone is a member of the same PCOL group and has a **PCOL** button.

Personal Status Access (PSA)

Using PSA, a user can execute a dissociate request from a bridged appearance. However, when a user executes a dissociate command at telephone B, the user dissociates from telephone B. This is the case, even if the user is on a bridged appearance that belongs to telephone A.

Priority Calling

The primary telephone user or the bridging user can make a priority call. If a priority call is made to an idle telephone, the primary telephone and all bridging users are alerted by priority alerting.

Privacy-Manual Exclusion

Activation of exclusion by any user (primary or bridged appearance) before placing a call, prevents any other user from bridging onto the call. Activation of exclusion by any user active on a call, while the primary user and/or any other bridging users are active on the call, drops all other users from the call (including the primary user), leaving only the activator and the calling/called party on the call.

Redirection Notification (multiappearance telephones only)

Redirection Notification is not provided at bridged appearances unless Ringing - Abbreviated and Delayed is administered to give notification.

Ringback Queuing

Ringback Queuing is not provided on calls originated from a bridged call appearance. However, after the primary user of the bridged extension has activated Ringback Queueing, the resulting callback call alerts at bridged appearances as well as at the primary user’s telephone. The call can be answered from the primary user’s telephone or from any bridged appearance.

Ringer Cutoff (multiappearance telephones only)

Ringer Cutoff prevents any nonpriority (or nonintercom) incoming call from ringing at that telephone. This is independent of whether the call is to the telephone's primary extension or to any of the bridged appearances' extensions.

Service Observing

You observe calls on a primary extension and all bridged appearances of that extension. You cannot observe bridged appearances on the extensions phone. 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.

The primary telephone user or bridging user can bridge onto a service observed call of the primary at any time. A bridging user cannot activate Service Observing using a bridged call appearance.

If the primary is service observing on an active call, a bridged call appearance cannot bridge onto the primary line that is doing the service observing.

Terminating Extension Group (TEG)

TEG calls to the primary extension do not ring at the associated bridged appearances. TEG calls cannot be answered or bridged onto from a bridged appearance. The primary telephone should not be assigned to a TEG.

Terminal Translation Initialization (TTI)

If a user is on a bridged appearance, the user cannot use TTI to separate from the telephone.

Transfer

Single-line telephones:

A call cannot be transferred by a single-line telephone if more than one user is active on that call.

The primary telephone user, when no other bridges are active on the call, can transfer the call using normal single-line transfer procedures. Any attempt by a bridging user to bridge onto this call during a successful transfer attempt is denied.

A single-line bridging user, alone on a bridged call, can transfer the call, using normal transfer procedures. Any attempt by the primary telephone user to bridge onto this call during a successful transfer attempt is ignored; and any attempt to bridge on by a bridging user is denied.

If the bridging user has no other available bridged appearances of the primary extension (other than the one he or she is currently on), the bridging user, after pressing the conference/transfer button, must select a call appearance to be used for the transfer, before dialing the number.

Multiappearance telephones:

If the bridging user has at least one available bridged appearance of the primary extension (other than the one he or she is currently on), the system automatically selects a bridged call appearance for the transfer when the conference/transfer button is pressed.

You can administer the system to automatically select the first idle appearance if there is no idle appearance with an extension matching the extension that is transferring the call.

If the primary user and the bridged user are both on the call when one user transfers the call, the user performing the transfer becomes the controlling user for the participation of both users on the conference. The controlling user is immediately dropped from the call. When the noncontrolling

user hangs up, the appearance goes on soft hold. In this case, one of two things must occur to disassociate the appearance from the call: all other parties on the call disconnect, or the controlling user rejoins the call and disconnects again.

Videophone 2500 (single-line telephones)

A user cannot use a single-line bridge to a Videophone 2500 principal that is on a video call.

Voice Message Retrieval

A voice message to the primary extension can be retrieved on a bridged appearance by the bridged appearance user. If a security code is required to retrieve the message, the bridging user must use the security code of the primary telephone.

Voice Paging

The use of Voice Paging automatically invokes exclusion. Therefore, interactions for this feature are the same as for Privacy-Manual Exclusion.

Chapter 48: Bulletin Board

Use the Bulletin Board feature to post information and retrieve messages from other users on the server. Avaya personnel can also leave high-priority messages on the bulletin board. The system displays the high-priority messages as the first 10 lines on the bulletin board.

Detailed description of Bulletin Board

Use the Bulletin Board feature to post information and retrieve messages from other users on the server. Anyone with an init or an inad login can add or change messages on the bulletin board. Avaya personnel can also leave high-priority messages on the bulletin board. The system displays the high-priority messages as the first 10 lines on the bulletin board.

When you log in to the system, the system alerts you to any messages that are on the bulletin board, and gives you the date of the last message.

If an Avaya employee enters a high-priority message while you are logged in, you receive the notification the next time that you enter a command. This high-priority message disappears after you enter a command. The system displays the high-priority message again each time that you log in, until you remove the message.

The bulletin board provides three pages of message space. You can write on any available line other than the high-priority lines.

You must maintain the bulletin board. If your bulletin board exceeds 80% capacity, the system displays the capacity that remains when you log in. If the bulletin board is full, the new messages overwrite the old messages.

Bulletin Board administration

The following steps are part of the administration process for the Bulletin Board feature:

- Setting user permissions
- Changing bulletin board information

Related links

Setting user permissions on page 327

Changing bulletin board information on page 327
Bulletin Board valid entries on page 328

Screens for administering Bulletin Board

Screen Name	Purpose	Fields
Command Permission Categories	Give permission to users to type nonpriority information on the Bulletin Board screen	• Display Admin and Maint Data • Administer Features
Bulletin Board	Add or change priority, or nonpriority, information in the system	All

Setting user permissions

Procedure

1. Type `change permissions` *`login ID`*, where *login ID* identifies the user who is to use the Bulletin Board feature. Press `Enter`.

   The system displays the Command Permission Categories screen.
2. In the **Display Admin. and Maint. Data?** field:
   - Type `y` if you want the user to:
     - Type nonpriority messages on the bulletin board
     - Use the display, list, monitor, status commands
     - Change his or her password
     - Schedule reports
3. In the **Administer Features** field:
   - Type `y` if you want the user to:
     - Type nonpriority messages on the bulletin board
     - Administer the feature-related parameters, such as coverage paths, class of service, class of restriction, system parameters, authorization codes, and security
4. Press `Enter` to save your changes.

Changing bulletin board information

Procedure

1. Enter `change bulletin-board`.

   The **date** field is a display-only field that contains the date that someone added or changed the line of information.

2. Type the bulletin board information.
   - Those who have an init or an inads login, including Avaya personnel, can type high-priority information in Line 1 through Line 10. High-Priority messages have an asterisk (*) at the beginning of the line. When someone with an init or an inads login types the high-priority information, the system displays the high-priority message the next time that you log into the system.
   - Those with permission, as defined on the Command Permission Categories screen, can type message information in:
     - Line 11 through Line 19 of Page 1
     - Line 1 through Line 20 of Page 2
     - Line 1 through Line 20 of Page 3
3. Select **Enter** to save your changes.

Bulletin Board valid entries

Table 6: Bulletin board entries

Character, number, or symbol	Symbol Name
A through Z	
a through z	
Blank	
0 through 9	
!	Exclamation mark
@	At sign
#	Pound sign
$	Dollar sign
%	Percent sign
^	Circumflex
&	Ampersand
*	Asterisk
_	Underscore
+	Plus sign
-	Minus sign or dash
=	Equal sign
[	Left bracket
]	Right bracket
{	Left brace
}	Right brace

Table continues…

Character, number, or symbol	Symbol Name
|	Bar or pipe
\	Back slash
‘	left single-quotation mark
’	right single-quotation mark or apostrophe
~	Tilde
;	Semi-colon
:	Colon
,	Comma
"	Right double-quotation mark
<	Left angle-bracket
>	Right angle-bracket
.	Period
/	Forward slash
?	Question mark

Considerations for Bulletin Board

This section provides information about how the Bulletin Board feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Bulletin Board under all conditions. The following considerations apply to Bulletin Board:

- Only users with an init or an inads login can add or edit high-priority messages.
- Only one user can change a message at a time.
- The bulletin board does not lose information during a system reset at level 1 or level 2. If you save translations, you can restore the information if a system reset occurs at levels 3, 4, or 5.

Chapter 49: Busy Indicator

Use the Busy Indicator feature to provide multiappearance telephone users and attendants with a visual indicator of the busy or the idle status of one of the following system resources:

- An extension number
- A trunk group
- A terminating extension group (TEG)
- A hunt group, either direct department calling (DDC) or uniform call distribution (UCD)
- Any loudspeaker paging zone, including all zones

Note:

A SIP phone can only support another extension.

Detailed description of Busy Indicator

You can assign extension numbers, trunk group access codes, and Loudspeaker Paging access codes to a **Busy Indicator** button.

The Busy Indicator button provides the attendant or the user with direct access to the extension number, the trunk group, or the paging zone.

The Facility Busy lamp indication for a Vector Directory Number (VDN) does not light when the VDN is being used. You can use the associated button to place a call to a VDN.

Busy Tone Disconnect

In some regions of the world, the Central Office (CO) sends a busy tone for the disconnect message. With Busy Tone Disconnect (BTD), the switch disconnects analog loop-start CO trunks when the CO sends a busy tone.

A call that originates from or terminates to a telephone that uses a BTD-enabled trunk has a Call Classifier port connected to the trunk. The Call Classifier port connects after the call is answered and stays connected on the trunk until the station hangs up, or a BTD signal is received from the CO. If only one BTD trunk is on a call when the BTD signal is received, the call is dropped. If the call is a conference call, only the trunk is dropped. The rest of the parties stay connected.

Interactions for Busy Indicator

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

Answer Supervision

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

Chapter 50: Busy Verification

Using the Busy Verification feature (**Verify** button), attendants and specific multiappearance telephone users can make test calls to trunks, telephones, and hunt DDC and UCD groups. Attendants and multiappearance telephone users can distinguish between a telephone that is truly busy and one that only appears busy because of some trouble condition. Users can also use this feature to quickly identify faulty trunks.

Detailed description of Busy Verification

An attendant or multiappearance telephone user can activate Busy Verify by pressing the **Verify** button. If they want to verify a telephone or hunt group, they enter an extension number. If they want to verify a trunk, they dial a trunk-access code, followed by the 2- or 3-digit number of the trunk-group member to be verified. If the trunk-group member number is less than 10, the system requires a leading zero (01 or 001 rather than 1).

After an attendant or multiappearance telephone user has activated Busy Verification, the system checks the validity of the extension or trunk-access code and member number. If the number is not a telephone extension, DDC/ UCD group-extension, ACD split number, or trunk access code with a valid member number, the system denies Verify and returns intercept tone.

When you use Verify to check a valid extension (one that is in the dial plan and assigned to a telephone), the system initiates a priority call to that extension. The table on page 332 describes the process.

Table 7: Verification of a telephone

Telephone Status	System Response	Result
Idle	• Generates priority ringing at the telephone. • Processes the call as a normal telephone-originated or attendant-originated call	• Verification is complete. • Anyone can place a call to the telephone.

Table continues…

Telephone Status	System Response	Result
Active on a call and has an idle call appearance	• Generates priority ringing at the first idle appearance. • Processes the call as a normal attendant-originated call.	• Verification is complete. • Anyone can place a call to the telephone extension.
Active on a call and has no idle call appearances or has only one line appearance	• Bridges the attendant onto the call. • Generates a warning tone to all active parties and repeats the tone every 15 seconds while the attendant remains bridged onto the call.	• Verification is complete. • The attendant can determine if the telephone is actually in use.
Out of service	• Generates reorder tone.	• Verification is denied.

When you use Verify to check a valid ACD split, UCD group, or DDC group, the system initiates a priority call to that group. (Valid in this case means the split or group is translated and at least one member is logged in.) the table on page 333 describes the process.

Table 8: Verification of an ACD Split, UCD Group, or DDC Group

Split or Group Member Status	System Response	Result
Available for an incoming call	• Generates priority ringing at the member's telephone. • Processes the call as a normal attendant-originated call.	• Verification is complete. • Anyone can place a call to the member's telephone.
All activated Make Busy	• Generates reorder tone.	• Verification is denied.
Not available for incoming calls	• The system does not queue the call even if a queue is available. • Generates reorder tone.	• Verification is denied.

When you use Verify to check a valid trunk, the system checks the status of that trunk. (Valid in this case means the trunk is translated with members and is not in an out-of-service state.) the table on page 333 describes the process.

Table 9: Verification of a Trunk

Trunk Status	System Response	Result
The trunk is idle and incoming.	• The system generates confirmation tone.	• Verification is complete. • Anyone can use the trunk.
The trunk is idle and outgoing.	• The system generates dial tone.	• Verification is complete. • Anyone can use the trunk.

Table continues…

Trunk Status	System Response	Result
The trunk is busy with an active call.	• The system bridges the Verify originator onto the call. • The system generates a warning tone to all active parties and repeats the tone every 15 seconds while the Verify originator remains bridged onto the call.	• Verification is complete. • The trunk is in use.
The trunk is out of service.	• The system generates reorder tone.	• Verification is denied.

Call log support for busy 94xx deskphones

Communication Manager 6.3.2 and later records all incoming calls when a 94xx deskphone is busy due to the following conditions:

- All but one call appearances reserved for incoming calls are in the non-idle state. The last call appearance is reserved for outgoing calls.
- All call appearances are in the non-idle state.
- The Do Not Disturb feature is active on the endpoint.
- One call appearance is busy on a call because a remote user has put the call on hold or started a transfer or a conference call.

Communication Manager records all missed calls in the missed call log of 94xx deskphones.

Busy Verification administration

The following tasks are part of the administration process for the Busy Verification feature:

- Assigning a Busy Verification feature button
- Activating the Busy Verify button

Related links

Assigning a Busy Verification feature button on page 335
Activating the Busy Verify button on page 335

Preparing to administer Busy Verification

Procedure

View the Trunk Group screen, ensure that the **Dial Access** field is set to `y`.

If this field is not set to `y`, go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Busy Verification, or to open a service request.

Screens for administering Busy Verification

Screen name	Purpose	Fields
Station	Set up busy verify extension	Feature Button Assignments

Assigning a Busy Verification feature button

Procedure

1. Enter `change station n`, where *n* is the station to be assigned the busy verify button.
2. In the **Feature Button Assignments** field, type `verify`.
3. Select **Enter** to save your changes.

Activating the Busy Verify button

Procedure

1. Press the **Verify** button on the phone.
2. Enter the Trunk Access code and member number to be monitored.

Considerations for Busy Verification

This section provides information about how the Busy Verification feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Busy Verification under all conditions. The following considerations apply to Busy Verification:

- A busy verification cannot be made to an analog extension that is waiting to be answered at another extension. A call must be answered before it can be verified.
- If your country requires a tone other than 440 Hz, use the Intrusion feature rather than Verify to verify telephones.
- The system does not provide bridging when you verify UCD and DDC groups or RLTs.
- You cannot make outgoing test calls on DID trunks.
- You can verify an extension that is administered without hardware (X-ported). In this case, the system generates reorder tone.

Interactions for Busy Verification

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

Automatic Callback

Once the called party in an Automatic Callback call hangs up, neither extension can be busy-verified until both the calling and called parties are connected or the callback attempt is canceled (by the activating party or by time-out of the callback interval).

Call Coverage

Since the busy-verification call to an extension is originated as a priority call, the call does not go to coverage.

Call Forwarding

Busy verification made to an extension with call forwarding activated, does not busy verify the forwarded-to extension. Only the called extension is busy verified.

Call Waiting Termination

You cannot verify an extension that called an active telephone and is receiving call-waiting ringback tone unless the extension has an idle call appearance.

Conference

The system denies busy verification of any extension involved in a conference call of more than five people. However, the system does allow a busy verification of any extension involved in a conference call of 5 or fewer parties. The system also denies busy verification of a trunk on a 6-party call.

Note:

For 12 parties to participate in a conference, you must enable the **12–party Conferences** field in the Feature-Related System-Parameters screen.

Data Privacy

Busy verification is denied if it would cause a bridging attempt on a telephone that has activated Data Privacy.

Data Restriction

The system denies Verify if Data Restriction is active on a call, and a busy verification bridging attempt is made on that call.

Hold

Busy verification of a multiappearance telephone is denied if all call appearances have calls on hold.

Individual Attendant Access

An attendant cannot make a busy verification of another individual attendant console or of the attendant group.

Loudspeaker Paging Access

The system denies busy verification if the telephone or trunk to be verified is connected to paging equipment.

Transfer

Once the originator of busy verification has bridged onto a call, any attempt to transfer the call is denied until the originator drops from the call.

Telephone Origination Restriction

A telephone that is origination restricted can be assigned a **Busy Verify** button. However, the button cannot be used.

Telephone Termination Restriction

The system denies busy verification of telephones that are termination restricted.

Chapter 51: Call Charge Information

Use the Call Charge Information feature to determine the approximate charge for calls that are made on outgoing trunks.

Detailed description of Call Charge Information

Communication Manager provides two ways to know the approximate charge for calls made on outgoing trunks.

Advice of Charge

For ISDN trunks, Advice of Charge (AOC) collects charge information from the public network for each outgoing call. Charge advice is a number that represents the cost of a call. The system records the charge information as either a charging unit or a currency unit.

Periodic Pulse Metering

For non-ISDN trunks, Periodic Pulse Metering (PPM) accumulates pulses that are 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 on which charges are determined.

Call-charge information helps you to account for the cost of outgoing calls before you receive the call charges from your network provider. The ability to account for the cost of outgoing calls before you receive the call charges from your network provider is especially important in countries where telephone bills are not itemized.

You can also use the information about the cost of outgoing calls to give the cost of telephone calls to employees. The cost information of outgoing telephone calls can help users to manage their use of company telecommunications facilities. Note, however, that you cannot necessarily use the call charge information that the Call Charge Information feature provides to reconcile telephone bills with your network provider.

You must request either AOC service or PPM service from your network provider. In some areas, your selection is limited. Note that the public network does not offer AOC service and PPM service in some countries, including the US. In some countries, AOC information is received automatically for each call. In other countries, the system must request AOC information for each call. Your Avaya representative can help you determine the type of service that you need.

In some countries, the public network sends call-charge information only at the end of a call. In other countries, the public network sends information both at the end of the call and while the call is in progress. PPM is available over the following trunk types:

- Central office (CO)
- Direct inward and outward dialing (DIOD)
- Foreign exchange (FX)
- Personal Central Office Line (PCOL)
- Wide Area Telecommunications Service (WATS)

Charge Display

With Communication Manager, you can view call charge information on a telephone display, or on a Call Detail Recording (CDR) report.

Charge Display at a user telephone

You can allow users to view call charges on telephone displays. From a display, a user can see the cost of an outgoing call, both while the call is in progress and at the end of the call. If you want users to control when the display of the call charge information, you can assign a display button that the user can press to see the current call charges. You can also administer the system so that the system displays call charges automatically whenever a user places an outgoing call.

Charge Display on a CDR report

You can administer the system to display call charges on CDR reports. For more information, see the “Call Detail Recording” feature.

Either the **ISDN C C** field or the **PPM** field in the CDR record contains the last cumulative charge received from the network. If Call Splitting or Attendant Call Recording is enabled, and a call is transferred for the first time, the **ISDN Call Charge** field contains the cumulative charge that was most recently received from the network.

For all subsequent transfers, the **ISDN Call Charge** field contains the difference between the cumulative charge that was most recently received and the value that was generated in the previous CDR record for the same call.

The system displays a zero in the **Call Charge** field when:

- No AOC information is received
- A value of zero is the last charge information that was received
- The outgoing trunk group is not administered for AOC or PPM

Call Charge Information administration

The following tasks are part of the administration process for the Call Charge Information feature:

- Administering the charge display
- Administering a trunk group for call charge displays
- Assigning a call charge display button for a user
- Assigning a call charge display feature button for an attendant
- Administering AOC for ISDN trunks
- Administering PPM for non-ISDN trunks
- Administering PPM for DS1 media module

Related links

Administering the charge display on page 343
Administering a trunk group for call charge displays on page 343
Assigning a call charge display button for a user on page 344
Assigning a call charge display feature button for an attendant on page 345
Administering AOC for ISDN trunks on page 345
Administering PPM for non-ISDN trunks on page 346
Administering PPM for DS1 media module on page 346

Preparing to administer Call Charge Information

Procedure

1. Define CDR to support Call Charge information.
2. Specify the frequency of the call charge displays.
3. Translate the Call Charge text.
4. Assign a COR for charge displays.

Related links

Defining CDR to support Call Charge Information on page 340
Specifying the frequency of the call charge displays on page 341
Translating the text “Call Charge” on page 341
Assigning a COR for charge displays on page 341

Defining CDR to support Call Charge Information

Procedure

1. Type `change system-parameters cdr`. Press `Enter`.

   The system displays the CDR System Parameters screen.
2. Administer the CDR System Parameters screen.

   For more information, see the Call Detail Recording feature.

Related links

Call Detail Recording on page 384

Specifying the frequency of the call charge displays

Procedure

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

   The system displays the Feature-Related System Parameters screen.

2. In the **Charge Display Update Frequency (seconds)** field, type the number of seconds between the charge update information displays that a user sees.

   The valid entries are 10 through 60, and blank.

   Note:

   Frequent display updates can have an impact on the performance of the system. If the duration of a call is less than the value in the **Charge Display Update Frequency (seconds)** field, the display does not automatically show the charge information.

   If you want a user to see the charge information, you must assign a **disp-chrg** feature button on the Station screen for a user.

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

Translating the text “Call Charge”

Procedure

1. Type `change display-messages miscellaneous-features`. Press `Enter`.
2. On the Language Translations screen, click `Next` until you see the translation number 47.
3. In the **Translation** field, type the translation for “Call Charge” if you need a translation for the text.
4. Press `Enter` to save your changes.

Assigning a COR for charge displays

Procedure

1. Type `change cor` *n*, where *n* is the number of the COR to which you want to assign an automatic charge display. Press `Enter`.

   The system displays the Class of Restriction screen.

2. In the **Automatic Charge Display** field, perform one of the following actions:

   - If you want the user to automatically see the call charges during a call and at the end of a call, type `y`.
   - If you want the user to press the disp-chrg feature button to see the call charges, type `n`. To see the call charges, the user must press the disp-chrg feature button before the system drops the call.

3. Press `Enter` to save your changes.

Screens for administering Call Charge Information

Screen name	Purpose	Fields
Attendant Console	Assign a feature button for the attendant to display charges	**Feature Button Assignments** area • disp-chgs
CDR System Parameters	Define Call Detail Recording (CDR) for the system	All
Class of Restriction	Specify a Class of Restriction (COR) that automatically displays the charges to the users	Automatic Charge Display
DS1 Media Module	Specify the values and the increments for Periodic Pulse Metering (PPM)	• Received Digital Metering Pulse Maximum • Received Digital Metering Pulse Minimum • Received Digital Metering Pulse value
Feature-Related System Parameters	Specify the frequency of the system displays for charge information	Charge Display Update Frequency
Language Translations	Specify a translation of the “Call Charge” text display	Call Charge
Station	Assign a feature button for the user to display charges	Feature Button • disp-chrg
	Assign a COR for an automatic display of call charges	COR
Trunk Group (all types)	Specify charge information that controls Call Charge Information processes and displays	• Charge Conversion • Charge Type • Currency Symbol • Decimal Point

Table continues…

Screen name	Purpose	Fields
Trunk Group • central office (CO) • Direct inward and outward dialing (DIOD) • foreign exchange (FX) • Personal Central Office Line (PCOL) • Wide Area Telecommunications Service (WATS)	Administer PPM for a non-ISDN network	• CDR Reports • Direction • Frequency • Outgoing Glare Guard (msec) • PPM
Trunk Group-ISDN-PRI	Administer Advice of Charge (AOC) for an ISDN network	• Charge Advice • Service Type • Supplementary Service Protocol • CDR Reports

Administering the charge display

Procedure

1. Administer a trunk group for call charge displays.
2. Assign a call charge display button for a user.
3. Assign a call charge display feature button for an attendant.

Administering a trunk group for call charge displays

Procedure

1. Type `change trunk-group n`, where *n* is the number of the trunk group for which you want to administer call charge display information. Press `Enter`.
2. On the Trunk Group screen, click `Next` until you see the **Charge Conversion** field.
3. In the **Charge Conversion** field, type the charge unit for the currency that you use.

   Valid entries are 1 to 64,500.

   The software multiplies the number of charge units by the value of the **Charge Conversion** field, and displays the result as a currency. If the **Charge Conversion** field is blank, the software displays the number of charge units, but does not convert the charge units to a currency.

   - The system displays the **Charge Conversion** field for central office (CO), direct inward and outward dialing (DIOD), foreign exchange (FX), and Wide Area Telecommunications Service (WATS) trunk groups when the **Direction** field on the Trunk Group screen is set to outgoing or two-way.

- The system displays the **Charge Conversion** field for ISDN trunk groups when the **Charge Advice** field on the Trunk Group screen is not set to none.

4. In the **Charge Type** field, type the words or the characters that you want the system to display after the system displays the call charge amount.

   You can leave the field blank, or you can type one to seven characters. The system counts a leading space, or an embedded space, as a character.

   - The system displays the **Charge Type** field for CO, DIOD, FX, and WATS trunk groups when the **Direction** field on the Trunk Group screen is set to outgoing or two-way.
   - The system displays the **Charge Type** field for ISDN trunk groups when the **Charge Advice** field on the Trunk Group screen is not set to none.

5. In the **Currency Symbol** field, type the symbol that you want the system to display before the system displays the call charge amount.

   You can leave the field blank or you can type one to seven characters. The system counts a leading space, or an embedded space, as a character.

   - The system displays the **Currency Symbol** field for CO, DIOD, FX, and WATS trunk groups when the **Direction** field on the Trunk Group screen is set to outgoing or two-way.
   - The system displays the **Currency Symbol** field for ISDN trunk groups when the **Charge Advice** field on the Trunk Group screen is not set to none.

6. In the **Decimal Point** field, type the representation of a decimal point that is appropriate for your currency.

   You can type `comma`, `period`, or `none`.

   If you type `comma` or `period`, the system divides the call charge amount by 100.

   - The system displays the **Decimal Point** field for CO, DIOD, FX, and WATS trunk groups when the **Direction** field on the Trunk Group screen is set to outgoing or two-way.
   - The system displays the **Decimal Point** field for ISDN trunk groups when the **Charge Advice** field on the Trunk Group screen is not none.

7. Press `Enter` to save your changes.

Assigning a call charge display button for a user

Procedure

1. Type `change station` *n*, where *n* is the extension of the user to whom you want to assign a call charge display feature button. Press `Enter`.

   The system displays the Station screen.

2. In the **COR** field, type the number of the COR that supports the automatic display of call charges.
3. Click `Next` until you see the **Button Assignments** area of the Station screen.

4. In the **Button Assignments** area, type `disp-chrg` next to the feature button number that you want the user to use to display a call charge amount.
5. Press `Enter` to save your changes.

Assigning a call charge display feature button for an attendant

Procedure

1. Type `change attendant` *n*, where *n* is the number of the attendant console to which you want to assign a charge display feature button.

   The system displays the Attendant Console screen.
2. Click `Next` until you see the **Feature Button Assignments** area.
3. In the **Feature Button Assignments** area, type `disp-chrg` next to the feature button number that you want the attendant to use to display a call charge amount.
4. Press `Enter` to save your changes.

Administering AOC for ISDN trunks

Procedure

1. Type `add trunk-group next`. Press `Enter`.
2. On the Trunk Group screen, click `Next` until you see the **Charge Advice** field.
3. In the **Charge Advice** field, perform one of the following actions:
   - If your public network sends AOC automatically, type `automatic`.
   - If the system must request charge information for each call, and you want to receive only the final call charge, type `end-on-request`.
   - If the system must request charge information for each call, and you want the system to display call charges both during the call and at the end of the call, type `during-on-request`.

     You can change this field from the default value of none, only if the **CDR Reports** field is set to `y`.
4. In the **Service Type** field, type `public-ntwrk`.
5. In the **Supplementary Service Protocol** field, type the supplementary service protocol that this trunk uses.
6. In the **CDR Reports** field, type the entry that provides the CDR information that you want for your system.
7. Press `Enter` to save your changes.

Administering PPM for non-ISDN trunks

Procedure

1. Type `change trunk-group n`, where *n* is the number of the trunk-group for which you want to administer PPM. Press `Enter`.

   The system displays the Trunk Group screen.

2. In the **CDR Reports** field, type the entry that specifies the circumstances under which you want the system to generate CDR report information.

3. In the **Direction** field, perform one of the following actions:

   - If you want this trunk to be used for incoming traffic, type `incoming`.
   - If you want this trunk to be used for outgoing traffic, type `outgoing`.
   - If you want this trunk to be used to network call redirection, type `two-way`.

     The system displays this field for all trunk groups except direct inward dialing (DID) and customer-premises equipment (CPE).

4. In the **Glare** field, type the minimum acceptable interval, in milliseconds, between the time that the server sends an outgoing seizure request and when the server receives a seizure acknowledgment.

   If the interval in which the server receives an acknowledgment is less than the interval that you specify in this field, glare is assumed. Valid entries are the numbers 40 to 100, in increments of 10.

   Only TN2140 ports receive this timer.

   You can administer this field only if the **Trunk Type** field is set to `cont`, and the **Direction** field is set to `two-way` or `outgoing`.

5. In the **Frequency** field, type the PPM pulse frequency that the public network requires.

   The system displays this field only if the **Direction** field is set to `outgoing` or `two-way`, and the **PPM** field is set to `y`.

6. In the **PPM** field, type `y`.

7. Press `Enter` to save your changes.

Administering PPM for DS1 media module

Procedure

1. Type `change ds1 n`, where *n* is the number of the DS1 media module for which you want to administer PPM. Press `Enter`.

   The system displays the DS1 Media Module screen.

2. In the **Received Digital Metering Pulse Maximum (ms)** field, type the number that your network service provider recommends.

Valid entries are 20 to 1000, in increments of 10. The number that you type in this field must be greater than the number that you type in the **Received Digital Metering Pulse Minimum (ms)** field.

The system displays this field only when the **Signaling Mode** field is set to `cas`, the **Interconnect** field is set to `co` or `pbx`, and the **Country Protocol** field is set to a protocol that uses PPM as defined in Country protocol codes for incoming digital PPM signaling on page 347.

3. In the **Received Digital Metering Pulse Minimum (ms)** field, type the number the number that your network service provider recommends.

   Valid entries are 20 to 1000, in increments of 10. The number that you type in this field must be less than the number that you type in the **Received Digital Metering Pulse Maximum (ms)** field.

   The system displays this field only when the **Signaling Mode** field is set to `cas`, the **Interconnect** field is set to `co` or `pbx`, and the **Country Protocol** field is set to a protocol that uses PPM as defined in Country protocol codes for incoming digital PPM signaling on page 347.

4. In the **Received Digital Metering Pulse Value** field, type the number that your network service provider recommends.

   Valid entries are 1 and 2.

   The system displays this field when the **Signaling Mode** field is set to cas, the **Country Protocol** field is set to 21, and the **Interconnect** field is set to co or pbx.

5. Press `Enter` to save your changes.

Country protocol codes for incoming digital PPM signaling

Table 10: Country protocol codes for incoming digital PPM signaling

Code	Country	PPM Min. (ms)	PPM Max. (ms)	PPM value
0	null	NA	NA	NA
1	US	NA	NA	NA
2	Australia	80	180	0
3	Japan	NA	NA	NA
4	Italy	120	150	1
5	Netherlands	90	160	0
6	Singapore	NA	NA	NA
7	Mexico	20	180	1
8	Belgium	20	180	1
9	Saudi Arabia	NA	NA	NA

Table continues…

Code	Country	PPM Min. (ms)	PPM Max. (ms)	PPM value
10	UK	NA	NA	NA
11	Spain	20	220	0
12	France	NA	NA	NA
13	Germany	NA	NA	NA
14	Czech Republic	20	420	1
15	Russia CIS	NA	NA	NA
16	Argentina	10	180	1
17	Greece	100	180	1
18	China	NA	NA	NA
19	Hong Kong	NA	NA	NA
20	Thailand	20	180	1
21	Macedonia Croatia	120 20	180 80	1 1
22	Poland	100	150	0
23	Brazil	NA	NA	NA
24	Nordic	NA	NA	NA
25	South Africa	160	240	0, 1

End-user procedures for Call Charge Information

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Displaying call charge information

Procedure

Press the **disp-chrg** button before the call drops.

If you press the:

- Elapsed-timer button, the elapsed-timer information can overwrite part of the call charge information.
- Local-directory-number button, the call charge information overwrites the directory number information.
- Exit or Normal button, the directory number information no longer overwrites the local directory number information.

Considerations for Call Charge Information

This section provides information about how the Call Charge Information feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Charge Information under all conditions. The following considerations apply to Call Charge Information:

Performance impact

Call Charge Information can have an impact on system performance in several ways. The information that comes in over ISDN trunks takes up bandwidth, and reduces the maximum amount of traffic that the ISDN D-channel can handle. This is especially true in countries such as Germany and France, where the network sends charging information updates as often as every 3 to 10 seconds for each active international call.

The number of telephones that display charge information and the frequency of updates also affect performance. Usually, the update frequency matches the average rate at which call charge updates are received from the public network.

⚠ Caution:

When users update displays too frequently, unnecessary system performance degradation can occur. If performance slows to an unacceptable rate, you can lengthen the amount of time between updates.

Interactions for Call Charge Information

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

Attendant Features

Attendant consoles cannot have an automatic charge display. If you want the attendant to see call charges, you must assign a **disp-chrg** button to the attendant console. If the attendant transfers an outgoing call, the display returns to normal mode. If the transfer is not completed, or the call remains at the attendant console, the attendant must press the disp-chrg button again to view call charges.

Automatic Incoming Call Display

If a user has charges displayed for an existing call, and a second call rings on another line appearance, the display returns to normal mode for a short time to show the identity of the caller. The user must press the disp-chrg again to view call charges. Or if automatic charge display is enabled, the user must wait for the Charge Display Update Frequency interval to expire.

Bridged Appearance

If a user uses a bridged call appearance to place a call, the system displays the call charges on the telephone from which the call is made. If Automatic Charge Display is part of the Class of Restriction (COR) for that telephone, the system displays the charges automatically. The system

displays the actual charge for the call on the Call Detail Recording (CDR) report as if the call was made from the principal extension, and not from the bridged appearance.

Call Coverage or Call Forwarding

Call charges for a call to an extension that the system redirects over a public network trunk, are charged to the called extension, not the calling extension. However, if the call is placed from an internal telephone that has charge display capability, the caller sees the charges for the redirected call.

Call Park

When a user parks a call, the display mode returns to normal. If a user retrieves a parked, outgoing call from another display telephone, the display on that set shows the current call charges if the user presses the disp-chrg button. The display also shows the charges if the Class of Restriction (COR) of the user supports Automatic Charge Display. If call splitting is enabled, the display shows the charges that accumulated since the user unparked the call.

Call Transfer

Advice of Charge (AOC) administration for the outgoing trunk group controls whether AOC information is requested or recorded for the call, when the system routes a transferred call over a public network ISDN-PRI trunk group. If two or more outgoing trunks are connected through trunk-to-trunk transfer, the software can receive AOC information from the network for each outgoing trunk that is involved in the call.

Call Detail Recording (CDR) Adjuncts

The software does not tandem AOC information through a private network to other switches. The CDR adjunct that records AOC information must receive its input from software that is directly connected to the public network.

CDR Call Splitting

- The system generates a separate call record, whenever the system transfers a call, if you administered CDR Call Splitting for outgoing trunks.
- Attendant Call Recording, which is a form of Call Splitting, generates a CDR record when an attendant drops from a call.
- Incoming Trunk Call Splitting has no effect on charge information.
- If you rely on Call Splitting or Attendant Call Recording, request call charge information during the call. However, if you use AOC, a request for call charge information during a call increases message activity on the signaling channel, and reduces Busy Hour Call Capacity.
- In some countries, or with specific protocols, AOC information is unavailable during a call. If AOC information in unavailable during a call, you can use the Elapsed Time in the CDR records to allocate the charges among the call participants.
- You must use CDR Call Splitting if you want the charge display to restart at zero when a call is transferred.

Centralized Attendant Services

In any configuration where a branch system has no direct connection to the public network, the private network does not pass call-charge information to these branches.

Conference

If a user adds a third party to a call that is in charge-display mode, the display returns to normal. The system does not display call charges when more than two parties are on the call.

Distributed Communications System (DCS)

In any configuration where a branch system has no direct connection to the public network, the private network does not pass call-charge information to these branches.

Electronic Tandem Network (ETN)

In any configuration where a branch system has no direct connection to the public network, the private network does not pass call-charge information to these branches.

Hold

If a user places a call on hold, the display returns to normal mode. The user must press the **disp-chrg** button again to view call charges. If the automatic charge display is enabled, the user must wait for the system to refresh the display.

Last Number Dialed

When a user is active on a call, a user can view the last number that the user dialed. To view the last number that was dialed, the user presses the stored-numb button, and then presses the last-numb button. To view call charges again, the user must press the **disp-chrg** button, or the **Normal** button if Automatic Charge Display is part of the COR of the user.

QSIG

In any configuration where a branch system has no direct connection to the public network, the private network does not pass call charge information to these branches.

System resets

If you perform a warm reset while calls are active with charge display, the charge display stops operating. To resume call charge updates, users must press the Normal button.

Chapter 52: CAC sharing between Communication Manager and Session Manager

With Call Admission Control (CAC) sharing between Communication Manager and Session Manager, Session Manager acts as the central authority for bandwidth management. Communication Manager gets bandwidth for voice and multimedia IP connections from Session Manager. You can set the limits for the bandwidth used by Communication Manager and other users through System Manager. For more information about setting bandwidth limits, see *Administering Avaya Aura® Session Manager*.

You can perform the following using this feature:

- Change bandwidth management.
- Add network region group.
- Assign each network region group to an IP network region.
- Map each network region group to a destination network region.
- Administer locations.
- Assign a network region group to an extension.

Enabling CAC sharing between Communication Manager and Session Manager

Procedure

1. On the Communication Manager SAT interface, run the following command: `change system-parameters ip-options`.
2. Navigate to the page that has the IP BANDWIDTH MANAGEMENT OPTIONS field.
3. In the **BW Management Option** field, type `shared-SM`.
4. In the **Signaling-group of Primary SM BW Mgr** field, type the SIP signaling group number of the primary Session Manager.
5. **(Optional)** In the **Signaling-group of Secondary SM BW Mgr** field, type the SIP signaling group number of the secondary Session Manager.

6. Save the changes.

Administering a network region group

Procedure

1. On the Communication Manager SAT interface, run the following command: `change network-region-group n`, where *n* is the network region group number.

   The system displays the NETWORK REGION GROUP page.

2. In the **Name** field, assign a unique name to the network region group.

   You can enter up to 20 alphanumeric characters. The name must be similar to the name of a location administered on System Manager at **Home** > **Elements** > **Routing** > **Locations**. While adding locations in System Manager, you must add the IP address of gateway and H.323 endpoint to the network region. For more information, see “Locations” section in *Administering Avaya Aura® Session Manager*.

3. Save the changes.

4. Add an extension and assign the network region to the extension.

Assigning a network region group to an IP network region

Procedure

1. On the Communication Manager SAT interface, run the following command: `change ip-network-region n`, where *n* is the IP network region number.

   The system displays the IP NETWORK REGION page.

2. In the **NR Group** field, assign the network region group number from `1` to `2000`.

   `1` to `250` are core network region groups and `251` to `2000` are stub network region groups.

   Multiple network regions can be assigned to the same network region group when multiple network regions share a common bandwidth pool and have unlimited bandwidth between them. For information about administering bandwidth, see “Locations” section in *Administering Avaya Aura® Session Manager*.

3. On the Inter Network Region Connection Management page, map the network region to the destination network region.

4. Save the changes.

Interactions for locations and network regions

Network regions can affect the following feature:

Emergency calling

For Session Manager managed bandwidth, emergency calls will always go through in spite of administered bandwidth limit exhaustion. If the emergency calls go through in spite of bandwidth limit exhaustion, bandwidth usage reporting on System Manager for the specific location may cross the administered bandwidth limit.

For information about administering bandwidth, see “Locations” section in *Administering Avaya Aura® Session Manager*.

Chapter 53: Call Coverage

Use the Call Coverage feature to automatically reroute incoming calls to alternate telephone numbers.

Detailed description of Call Coverage

Use Call Coverage to:

- Reroute incoming calls to alternate telephone numbers when the called party is unavailable to answer calls
- Establish the order in which calls are redirected to alternate destinations
- Establish up to six alternate destinations for an incoming call
- Establish redirection criteria that govern when the system redirects a call
- Establish multiple coverage paths that the system can select from based on redirection criteria
- Redirect calls based on the time of day
- Redirect calls to a local telephone number or to a telephone number in the public network
- Allow users to change their lead coverage path from both onsite and off-site locations

When a call meets the redirection criteria for a called telephone number, the system attempts to route the call sequentially to one of the points in a coverage path. Users can have a maximum of six points in the coverage path. If no coverage points are available, the call might revert to the original called number. If any point in the path is available, the call either rings at the individual telephone, an available member of a coverage group, or queues to the coverage group. Once a call is ringing or queued at any point in a coverage path, the call neither reverts to the original number, nor to the previous coverage point.

A call continues to ring at a coverage point for the interval that is administered for Coverage Subsequent Redirection. At the end of this interval, the system attempts to route the call to any points that remain in the coverage path. If no other point is available to accept the call, the call remains queued, or continues to ring at the current coverage point.

What is a Call Coverage path?

A call coverage path is a list of one to six alternate answering positions. The system sequentially accesses the coverage points when the called party or the called group is unavailable to answer the call.

When a call meets the redirection criteria for a called telephone number, the system attempts to route the call sequentially to one of the points in a coverage path. Users can have a maximum of sixpoints in the coverage path. If no coverage points are available, the call might revert to the original called number.

You can assign a coverage path to any of the following entities:

- An automatic call distribution (ACD) split
- An agent login ID
- A personal central office line (PCOL) group
- A Terminating Extension Group (TEG)
- A hunt group
- A telephone that can be either on site or off site

You define the coverage paths and establish the redirection criteria. You can include any of the following entities as points in a coverage path:

- A telephone number
- A voice messaging system
- An announcement
- An attendant group
- A uniform call distribution (UCD) hunt group
- A direct department calling (DDC) hunt group
- An ACD hunt group
- A coverage answer group (CAG)
- A vector directory number (VDN)

Multiple coverage paths

The system can select from multiple coverage paths that you define for a single destination. However, the system uses only one coverage path per call. The system first considers Coverage Path 1, the lead coverage path, when the system directs a call to coverage.

When the system redirects a call to coverage, the system checks the lead coverage path to determine whether the coverage redirection criteria of the path match the call status. If the criteria match, the system uses the lead coverage path. If the redirection criteria of the lead coverage path does not match, the system moves in sequence from point to point in the coverage path to find a coverage path with redirection criteria that matches the call status. If the system does not find

a match, the call remains at the called extension. Once the system selects a coverage path, that path is used throughout the duration of the call.

Call Coverage supports the following capabilities:

Call Coverage

The system reroutes incoming calls to alternate telephone numbers when the called party is unavailable to answer calls.

Call Coverage Off Network

You can administer and 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.

Call Coverage Time of Day

You can administer the redirection of calls to different lead coverage paths based on the day of the week and the time of day.

Call Coverage Changeable Coverage Paths

Users can use a Feature Access Code (FAC) to modify coverage points.

Consult

Users can answer a coverage call, and then communicate with the called user without the caller hearing the conversation.

Time-of-Day Coverage

Use the Time-of-Day Coverage capability to redirect calls to different lead coverage paths at different times of the day, and on different days of the week.

For example, a user might want incoming calls to go to coverage based on the following schedule:

- To a co-worker at the office during normal business hours
- To an off-network destination, such as home, in the early evening
- To a voice messaging, such as Communication Manager Messaging, at all other times

To provide the user with the requested coverage, you administer the information in the table on page 357.

Table 11: Example of a Time-of-Day coverage table

Day of the week	Time 1 directed to	Time 2 directed to	Time 3 directed to	Time 4 directed to
Monday	00:00 CovPath3 (Communication Manager Messaging)	08:00 CovPath1 (Office)	17:30 CovPath2 (Home)	20:00 CovPath3 (Communication Manager Messaging)

Table continues…

Day of the week	Time 1 directed to	Time 2 directed to	Time 3 directed to	Time 4 directed to
Tuesday	00:00 CovPath3 (Communication Manager Messaging)	08:00 CovPath3 (Office)	17:30 CovPath3 (Home)	20:00 CovPath3 (Communication Manager Messaging)
Wednesday	00:00 CovPath3 (Communication Manager Messaging)	08:00 CovPath1 (Office)	17:30 CovPath2 (Home)	20:00 CovPath3 (Communication Manager Messaging)
Thursday	00:00 CovPath3 (Communication Manager Messaging)	08:00 CovPath3 (Office)	17:30 CovPath3 (Home)	20:00 CovPath3 (Communication Manager Messaging)
Friday	00:00 CovPath3 (Communication Manager Messaging)	08:00 CovPath1 (Office)	17:30 CovPath2 (Home)	20:00 CovPath3 (Communication Manager Messaging)
Saturday	00:00 CovPath3 (Communication Manager Messaging)			
Sunday	00:00 CovPath3 (Communication Manager Messaging)			

The Time-of-Day Coverage table represents time in 24-hour format. Activation times are ascending from the earliest to the latest. The activation times cover the entire day. If you do not assign a lead coverage path to a specific time interval, no coverage exists from that time until the next activation time.

When a call arrives at an extension, the system determines the lead coverage path that is in effect at that time. The system uses the information to redirect the call. If you change call coverage for a user while the user has a call in progress, your changes do not affect the call in progress.

Off-network Call Coverage

You can use standard remote coverage to an external number to send a call to an external telephone. However, the system does not monitor the call once the call leaves your system. Therefore, if the call is busy or not answered at the external number, the call cannot be directed back to the system.

Note:

Using remote coverage, you cannot cover calls to a remote voice mail.

Using the Coverage of Calls Redirected Off Net (CCRON) capability, you can use an external number in a coverage path. The system monitors the call to determine whether the external

number is busy or unanswered. If necessary, the system can redirect a call to coverage points that follow the external number. Any coverage point can be an off-network destination.

Use this capability for a call to follow a coverage path that:

1. Starts at the called extension
2. Redirects to the home telephone, and if unanswered at home
3. Returns to the voice mail box of the called extension

Note that the call does not return to the system if the external number is the last point in the coverage path, except when no trunks are available to route the call. In that case, the system attempts to again terminate the call at the original called extension.

When the system redirects an incoming trunk call off the network, a timer is set. The timer prevents the system from redirecting other incoming trunk calls from redirecting off the network until the timer either expires or is cancelled. The timer prevents calls that were redirected off the network from being routed back to the original telephone number from the off-network destination. Calls that are routed back to the original telephone number in this situation effectively create a loop that seizes trunks until trunks are no longer available.

The system provides the means to perform call classification on an off-network coverage call to determine the disposition of the call. If the off-network call is carried completely over ISDN facilities to the final destination, ISDN trunk signaling is used to monitor the call. If ISDN trunk signaling is not used to monitor the call, a call classifier port is used to cancel the call.

When the system tries to use a call classifier port to classify an off-network coverage call, the system introduces an unavoidable cut-through delay while the call classifier port attempts to identify an answered call. Neither the originating party nor the answering party hears each other during the 1-second or less delay. A call classifier is attached to all off-network coverage calls, that are made over analog facilities or over ISDN facilities, if the call is interworked to non-ISDN facilities on the public network.

When you enable CCRON:

- The system monitors off-network calls and returns the calls to the system if the calls are not answered within the administered time interval. Calls also return to the system if the system detects a call progress tone, such as busy or reorder.
- A simulated bridge appearance (SBA) is put on the called extension, and the green lamp flashes. A user can answer the call at the called extension at any time.
- When the system uses a call classifier port to classify the call, the system plays local ringback tone to the caller while the system is classifying the off-network call. The system uses the local ringback tone so that the user does not hear what is happening on the public network. As a result, the calling party will not hear the first few syllables that the answering party speaks.
- If any party on the call is on hold when the system routes the call off the network, the call classifier is removed from the call. The call behaves as if CCRON is not enabled.
- While an off-network call is undergoing call classification, any party that is not already on the call cannot bridge onto the call. Also, the originating party cannot release the call, conference anyone else onto the call, or transfer the call to a new party. Once the call is answered at an

off-network destination, or the call is returned to the system for further call processing, these restrictions are removed.

- If the last point in a coverage path is an off-network destination and no trunks are available to route the call, the system attempts to again terminate the call to the called extension.
- The system has no control over any redirection of the call that might take place at an off-network destination. However, further coverage treatment is provided if the off-network redirection interval expires before the call is answered at an off-network destination.

Call Coverage changeable coverage paths

With the changeable coverage path capability, users can use a Feature Access Code (FAC) to modify coverage paths.

Extended User Administration of Redirected Calls capability

Using the Extended User Administration of Redirected Calls capability, users can change the lead coverage path or the call forwarding destination from any onsite or off-site location. This capability is also known as remote access. For more information, see the Extended User Administration of Redirected Calls feature.

Related links

Extended User Administration of Redirected Calls on page 736

Call coverage criteria

Coverage criteria determine the conditions when the system redirects a call from the called extension to the first position in the coverage path. The Call Coverage feature provides the following coverage criteria:

Active

Redirects calls to coverage immediately when the called extension is active on at least one call appearance. For a telephone with only one appearance or a single-line extension, assign the Busy criterion instead of the Active criterion.

Busy

Redirects calls to coverage when all available call appearances at the called extension are in use.

The system redirects an incoming call, other than a priority call, to coverage only when all call appearances are in use.

A TEG is considered busy if any telephone in the group is active on a call.

Each telephone in a UCD group or a DDC group must be active on at least one call appearance for the system to redirect a call to coverage. If any telephone in the group is idle, the system directs the call to the idle telephone. If no telephone is available, the call can queue, if queuing is provided. If queuing is not provided, the system routes the call to coverage. If the queue is full or all agents are in an AuxWork mode, the system routes the call to coverage. Queued calls remain in the queue for the specified interval.

A call does not cover to a hunt group if no agents are logged in, or if all agents are in AuxWork mode.

Don’t Answer

Redirects calls to coverage if the calls are unanswered during a specified interval. A call rings for the specified number of seconds, and then the system redirects the call to coverage.

Cover All Calls

Redirects all incoming calls to coverage. This criterion has precedence over any other previously assigned criterion.

Send All Calls/Go to Cover

Users can activate Send All Calls or Go to Cover as overriding coverage criteria. You must assign this redirection criteria before a user can activate Send All Calls or Go to Cover.

No Coverage

Occurs when no coverage criteria are assigned. The system redirects calls to coverage only when the call extension activates Send All Calls, or the caller activate Go to Cover.

You can combine Active/Don’t Answer and Busy/Don’t Answer coverage criteria. Other combinations are either impossible or ineffective.

You assign redirection criteria separately for internal and external calls. You can link coverage paths so that you can assign Busy Don’t Answer for internal calls, and Active for external calls. Similarly, you can assign Busy/Don’t Answer for external calls, and No Coverage for internal calls. When you assign No Coverage for internal calls, internal calls remain directed to the called telephone or the called group.

All calls that are extended by the attendant are treated as external.

Enhanced Redirection Notification

The redirection features available in Communication Manager Release 5.2 and later include Do Not Disturb, Send All Calls, and Call Forwarding. The activation of redirection features at a user’s station is indicated through visual display or through a special dial tone (if the station is not equipped with a display). This feature works on DCP and IP (H.323) telephones, but not on IP (SIP) telephones and attendant consoles.

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

Detailed description of Enhanced Redirection Notification

The system uses Enhanced Redirection Notification to display the status of redirection features, selected posted message, and date and time information.

- Do Not Disturb

- Send All Calls
- Call Forward
- Selected Posted Message
- LNCC
- Enhanced Call Forward
- Station lock

If there are multiple status messages, the active features are displayed on scrolling, in the order of decreasing priority. The date and time information is displayed at the end of the loop and has the lowest priority, but is displayed for twice as long as any of the other status messages. If **Scroll Status messages Timer (sec.)** is set to blank, scrolling is disabled, and only the feature with the highest priority is displayed. When no feature is active, only the date and time information is displayed. To guard against loading the system with status messages, the scrolling is started randomly. For example, when the user releases the handset for the first time.

Note:

After activation or deactivation of the feature, the display might remain unchanged until the first user interaction, such as going on-hook.

Limitations of Enhanced Redirection Notification

Enhanced Redirection Notification applies only when a station is idle and in normal display mode (not displaying a crisis alert or directory.) Enhanced Redirection Notification does not work if ringing is prevented at the station through use of Silent Ringing, Ringing Abbreviated/Delayed, or Per Button Ring Control. If the redirection number to be displayed does not fit into the display because the number is too long (18 digits or more), the standard scroll applies.

Enhanced coverage and ringback for logged off IP/PSA/TTI stations

To enable call coverage for logged off IP/PSA/TTI stations you must administer the **Criteria for Logged Off/PSA/TTI Stations** field on the System Parameters Call Coverage/Call Forwarding screen. The call then redirects to coverage after the number of rings exceed the number specified in the **Number of Rings** field for logged off IP/PSA/TTI coverage criteria.

This feature is supported for SIP endpoints from Communication Manager Release 7.1.

For more information about the **Criteria For Logged Off IP/PSA/TTI Stations**, **Logged off/PSA/TTI**, and **Number of Rings** fields, see *Avaya Aura® Communication Manager Screen Reference*.

VDN in a call coverage path (VICP)

If you assign a vector directory number (VDN) extension as the last point in a call coverage path, you apply call vectoring functionality to the coverage point. The programmable vector that is associated with the VDN provides flexibility in call handling.

You can program a vector that is assigned to the VDN in the coverage path to queue a redirected call to a messaging split for call answer operation, and to allow the caller to leave a message at

the called extension. The same VDN can also be used to retrieve messages. You can also vary the vector program by split status or time-of-day to provide different types of coverage.

When a redirected call covers to a VDN, the simulated bridged appearance of the called extension is removed when vector processing starts.

When covered calls or direct calls are connected to Communication Manager Messaging or to a messaging split through call vectoring, both the original reason for redirection and the called extension must be passed to the adjunct over the Switch Communication Interface (SCI) link.

Use of a VDN as a coverage point provides integration to Centralized Messaging. That is, the distributed communication system (DCS) message that is sent to the remote switch with Communication Manager Messaging includes the original reason for redirection and the called extension.

Coverage answer groups

You can create coverage answer groups of any type of SIP devices or non-SIP devices from 1 through 100. When calls are redirected to the group, members of the coverage answer group ring simultaneously. Anyone in the answer group can answer the incoming call.

Note:

The special application feature related to coverage answer groups, SA9123–Re-ring CAG Members in Adjacent Coverage Points, doesn't work with SIP phones.

Announcement in a coverage path

In general, do not assign an announcement as a point in a coverage path. When the system redirects a call to an announcement, the system plays the announcement and then drops the call. The system drops the call even if there are additional points in the coverage path.

You might want to use an announcement as the last point in a coverage path. The announcement could inform the caller that there is no one to answer the call and advise the caller to call back at another time. Keep in mind that the system drops the call once the system plays the announcement.

Hunt group in a coverage path

You can assign call coverage for a hunt group. If a hunt group queue is full, a call waits for a specified interval. The system then directs the call to the coverage path. The call coverage point can be another hunt group. A call does not cover to a hunt group if no agents are logged in, or if all agents are in AuxWork mode.

Subsequent redirection interval

The subsequent redirection interval controls the number of times that a call rings at a coverage point before the call moves to the next coverage point. The number of rings that the interval control depends on the type of coverage point. For example, the number of rings is different at a local coverage point and a remote coverage point.

Notifying users when the calls are redirected

You can administer a setting that notifies users when the users have a capability active that might redirect the calls. For example, if send all calls or call forwarding is active for a user, you can administer a setting to play a special dial tone when the user goes off hook.

Caller response interval for call coverage

The system uses a single, short tone, called a “redirect” tone, to inform an internal calling party (including incoming trunk calls from DCS and QSIG-VALU trunk groups) that the system is redirecting a call to coverage. The redirect tone is followed by an optional period of silence, called the Caller Response Interval. During this interval, the calling party has time to decide whether to:

- Disconnect
- Activate Priority Calling (this overrides coverage and re-rings the called party with a special ringing tone)
- Activate Leave Word Calling (LWC)
- Activate Automatic Callback
- Activate Go to Cover (this cancels the remaining Caller Response Interval and rings the first available coverage point)

Note that each of the above features except Go To Cover is available both locally on a single server, as well as over DCS and QSIG-VALU. The ability for the calling party to hear the redirect tone does not require the optional feature “DCS Call Coverage”; it is part of basic DCS.

Administer the redirect tone on page 2 of the Tone Generation screen (**`change tone-generation`**) by selecting redirect in the **Tone Name** field.

Note:

If the majority of the calls on your system go directly to voice mail without first covering to another party, and if features such as Leave Word Calling, Automatic Callback, Go To Cover, and Priority Calling are rarely used, it is advisable to reduce the length of this interval from its default value of 4 seconds, since this timer increases the delay before the voice mail system answers the call.

Consult

When a user answers a coverage call, the user can communicate with the called user without the caller hearing the conversation. This is called “private consultation”. To consult privately with the called user, the covering user presses the **Transfer** button, and then the **Consult** button. When the covering user presses the **Transfer** button, and then the **Consult** button, the system places the caller on hold. The system then establishes a connection between the called user and the covering user.

The covering user can create a conference call between the called user, the covering user, and the caller.

The covering user can transfer the call back to the called user.

The system maintains a Consult call at a Temporary Bridged Appearance, if a Temporary Bridged Appearance is available. If a Temporary Bridged Appearance is unavailable, the system uses any idle call appearance for the Consult call. If an idle call appearance is unavailable, the system denies the Consult call.

Features that override Call Coverage

Some features override Call Coverage criteria. The system checks the criteria of the overriding features before the system checks the coverage criteria. The following features override Call Coverage:

Call Forwarding (All Calls, Busy-Don’t Answer, Enhanced)

The Call Coverage feature skips a coverage point if that coverage point has any form of call forwarding activated. This includes a scenario, where a member of a Coverage Answer Group has call forwarding activated, that member does not ring when a call is routed to the Coverage Answer Group.

Call Forwarding All Calls

Call Forwarding All Calls temporarily overrides the redirection criteria if Send All Calls is inactive. The system attempts to complete the call at the forwarded-to extension before the system redirects the call to coverage. If the redirection criteria of the called extension are met at the forwarded-to extension, the system redirects the call to the coverage path of the called extension.

Go to Cover

Users can use Go to Cover to send a call directly to coverage, when the users call an internal extension. The internal calling party activates Go to Cover, and can assign Go to Cover to a telephone.

Send All Calls

Users can use Send All Calls to temporarily direct all incoming calls to coverage, regardless of the coverage criteria that are assigned to their extension. With this feature, users can also temporarily remove their telephones from the coverage path of another user.

A user cannot activate Send All Calls, if Send All Calls is excluded from the coverage criteria of the extension.

Send All Calls does not affect TEG calls.

Send Term

Send Term is the TEG equivalent of Send All Calls. Since a TEG cannot be in a coverage path, Send Term applies only to a TEG that is called directly.

Conditions that override Call Coverage

Call Coverage redirects calls from the called extension or the called group to alternate answering positions when certain criteria are met. Sometimes calls are sent back to the called extensions or the alternate destination, even though the redirection or overriding criteria are met.

The following list contains the conditions that cause the system to override Call Coverage.

- If no answering positions are available in the overage path, the call rings at the called telephone, if possible. If the call cannot ring at the called telephone, the calling party receives busy tone. The calling party receives busy tone, even if the Cover All Calls redirection criterion or the Send All Calls overriding criterion is active.
- If the system redirects a call to a coverage point that is unavailable, the call goes to the next coverage point. The call goes to the next coverage point, regardless of the type of coverage that is administered in the coverage point that is unavailable.
- When UCD and DDC group members are unavailable to answer calls to the group, the calls go to a queue, if queuing is available. The call remains in the queue for the call response interval before the system routes the call according to the coverage path. If no points on the path are available, the call remains in the queue. When neither group queuing nor a coverage point is available, the caller receives a tone or ringback, depending on the type of trunk that carries the call.

  If the redirection criterion is Active or Cover All Calls, a called extension can receive a redirection notification signal when the system routes the call to coverage. The redirection notification signal is a short burst of ringing. You can administer the redirection notification signal option for any extensions in your system.

  Redirected calls maintain an appearance on the called telephone, if possible. The call appearance status lamp flashes to indicate an incoming call before the system attempts to redirect the call. When the system redirects the call, the status lamp continues to flash. If the system redirects the call to Communication Manager Messaging, the lamp goes out. If the call appearance is flashing, a user presses the call appearance button to answer the call. If a covering user answers the call, the called user can bridge onto the call. If a covering user answers the call, the status lamp on the telephone of the called user lights steadily.
- Telephone users use Directed Call Pickup to answer calls that ring at another telephone or calls that alert at a coverage point. A call alerts when a call causes a call appearance on the telephone to flash. Using the Directed Call Pickup feature, a user can answer an alerting call from any telephone on the system.
- The system routes the following types of calls to the telephone of the called user until the user activates Go to Cover:
  - Priority calls
  - Dial Intercom calls
  - Automatic Intercom calls

  The system gives these calls precedence over the redirection criteria, and seizes the call appearance that is usually reserved for outgoing calls, if no other call appearances are available.

Call Coverage administration

The following tasks are part of the administration process for the Call Coverage feature:

- Creating a coverage path
- Assigning a coverage path to a user
- Assigning a **Consult** button for a user
- Defining coverage redirected off-network calls
- Assigning time-of-day coverage
- Assigning Internal Alerting
- Enabling enhanced Redirection Notification

Related links

Creating coverage answer groups on page 375
Creating a coverage path on page 368
Assigning a Consult button for a user on page 372
Assigning a coverage path to a user on page 371
Defining coverage redirected off-network calls on page 372
Assigning time-of-day coverage on page 374
Assigning Internal Alerting on page 376
Enabling enhanced Redirection Notification on page 376

Preparing to administer Call Coverage

Procedure

1. Type `change feature-access-codes`. Press `Enter`.
2. On the Feature Access Codes (FAC) screen, click `Next` until you see the **Send All Calls Activation** field.
3. Type an FAC in the **Send All Calls Activation** field.
4. Type an FAC in the **Send All Calls Deactivation** field.

   For more information, see the “Feature Access Code” feature.
5. Press `Enter` to save your changes.

Screens for administering Call Coverage

Screen Name	Purpose	Fields
Call Coverage Answer Group	Establish answer groups	All

Table continues…

Screen Name	Purpose	Fields
Coverage Path	Establish points in the coverage path	All
Feature Access Code	Assign Feature Access Codes (FACs) to activate or deactivate coverage-related actions	• Send All Calls Activation • Send All Calls Deactivation
Hunt Groups	Establish groups of users who answer calls for each other	All
Remote Call Coverage Table	Assign the telephone numbers of remote coverage points	All
Station	Define coverage information and button assignments for the called user	• Coverage Path 1 • Coverage Path 2 • Redirect Notification • Button Assignments for goto-cover and send-calls
	Define button assignments for the user to whom the system redirects the call	Button assignments for do not disturb (dn-dst), go to cover (goto-cover), and send all calls (send-calls)
	Define the goto-cover coverage point	Button Assignment for goto-cover
System-Parameters Call Coverage/Call Forwarding	Enable the Call Coverage Off-Net capability	Coverage of Calls Redirected Off-Net Enabled
System-Parameters Features	Enable Enhanced Redirection Notification	REDIRECTION NOTIFICATION fields
Optional Features	Verify that the CCRON capability is active in your system.	Coverage of Calls Redirected Off-Net
Terminating Extension Group	Define the group of users who can answer a call that simultaneously alerts at the telephones of the group members	All
Time of Day Coverage Table	Assign coverage throughout the day and week	All
Trunk Group: • APLT • ISDN-PRI • Tie	Specify the internal ringing and call coverage used for incoming trunk calls	Internal Alert?

Creating a coverage path

Before you begin

Verify that the settings on the System-Parameters Call Coverage/Call Forwarding screen contain the values that you want for your system.

For basic Call Coverage, Avaya recommends that you retain the default settings. However, if you decide to change the default settings, read the field definitions and the field descriptions carefully before you make changes.

To view this screen, type `display system-parameters call coverage/call forwarding`. Press `Enter`.

For a complete description of the System-Parameters Call Coverage/Call Forwarding screen, see *Administering Avaya Aura® Communication Manager*.

Procedure

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

   The system displays the Coverage Path screen that shows the next undefined coverage path. The **Coverage Path Number** field is a display-only field.

   To see the extensions or the groups that use a specific coverage path, type `display coverage sender group n`, where *n* is the coverage path number. For example, you might want to see which extensions use a coverage path before you make changes to the coverage path.

2. In the **Hunt After Coverage** field, type `y` if you want the system to attempt station hunting from the last coverage point, when the coverage point is a busy station. If you do not want the system to attempt station hunting from the last coverage point when the coverage point is a busy station, leave the default set to `n`.

3. In the **Next Path Number** field, perform one of the following actions:

   - Type a coverage path number in the field if you want the system to redirect if the coverage criteria of the current path does not match the call status. If the coverage criteria of the next path matches the call status, the system uses the coverage criteria to redirect the call, and no other path is searched.
   - Leave the field blank if you do not want the system to redirect the call.

     Linkage is a display-only field that shows one or two assigned coverage paths that are linked to the number in the **Next Path Number** field.

4. Find the **Coverage Criteria** area.

   Note:

   There is a column for inside calls and a column for outside calls. You can accept the defaults for both columns or only one column. Likewise, you can change the defaults for both columns or only one column.

   Perform any of the following actions:

   - In the **Active** fields, perform one of the following actions:
     - Accept the default value n if you do not want the call to go to coverage if only one call appearance is busy.
     - Type `y` if you want the call to go to coverage if only one call appearance is busy.

- In the **Busy** fields, perform one of the following actions:
  - Accept the default value y if you want the call to go to coverage if the extension is busy.
  - Type `n` if you do not want the call to go to coverage if the extension is busy.
- In the **Don't Answer** fields, perform one of the following actions:
  - Accept the default value y if you want the call to go to coverage if the number of rings exceeds the number specified in the **Number of Rings** field.
  - Type `n` if you do not want the call to go to coverage if the number of rings exceeds the number specified in the **Number of Rings** field.
- In the **Number of Rings** field, type a number from 1 to 99. This number indicates the number of times a call rings at a telephone before the system redirects the call to the first coverage point. The default is 2.
- In the **All** fields, perform one of the following actions:
  - Accept the default value y if you want the users with this path to answer their own calls.
  - Type `n` if you do not want the users with this path to answer their own calls. These user calls always immediately go to coverage.
- In the **DND/SAC/Goto Cover** fields, perform one of the following actions:
  - Accept the default value y if you want users to activate Send All Calls, temporarily direct all incoming calls to coverage (regardless of the assigned Call Coverage redirection criteria), and to temporarily remove their telephone from the coverage path.
  - Type `n` if you do not want users to activate Send All Calls, temporarily direct all incoming calls to coverage (regardless of the assigned Call Coverage redirection criteria), and to temporarily remove their telephone from the coverage path.
- In the **Logged off/PSA/TTI** fields, perform one of the following actions:
  - Accept the default value y if you want the call to go to coverage if the number of rings exceeds the number specified in the **Number of Rings** field.
  - Type `n` if you do not want the call to go to coverage if the number of rings exceeds the number specified in the **Number of Rings** field.
- In the **Number of Rings** field, type a number from 1 to 99. This number indicates the number of times a call rings at a telephone before the system redirects the call to the first coverage point. The default is 2.
- In the **Terminate to Coverage Pts. with Bridged Appearances** field, perform one of the following actions:
  - Accept the default value n if you want a call to skip the coverage point if the call has already alerted as a bridged call.

- Type `y` to allow a call to alert as a bridged call and a redirected call.

5. In the **Point** fields, type the extensions, the hunt group number, or the coverage answer group numbers that you want for coverage points.

   When you type a number and move to the next **Point** field, the system displays the **Rng** field.

6. In the **Ring** field, perform one of the following actions:

   - Leave the **Rng** field blank if you want to use the number of rings entered in the **Number of Rings** field.
   - Type the number of rings for this coverage point if you do not want to use the number of rings entered in the **Number of Rings** field.

   Note:

   To enter an extension that is assigned as a vector directory number (VDN) as the last point in the coverage path, you must make an administration change. For more information, see *Avaya Aura® Call Center Elite Feature Reference*.

7. Press `Enter` to save your changes.

Assigning a coverage path to a user

Before you begin

You must complete the Creating a coverage path procedure before you can assign a coverage path.

Procedure

1. Type `change station n`, where *n* is the extension to which you want to assign a coverage path. Press `Enter`.
2. On the Station screen, click `Next` until you see the **Coverage Path 1** field.
3. In the **Coverage Path 1** field, type a coverage path number of a previously administered Call Coverage Path screen.
4. Perform one of the following actions:
   - In the **Coverage Path 2** field, type a coverage path number of a previously administered Call Coverage Path screen, if you want the extension to have an alternative coverage path.
   - Leave the **Coverage Path 2** field blank if you do not want a second coverage path.
5. Press `Enter` to save your changes.
6. Click `Next` until you find the **Redirect Notification** field.
7. In the **Redirect Notification** field, perform one of the following actions:
   - Accept the default value y if you want a half ring at the telephone when the system redirects a call to coverage.

- Type `n` if you do not want the half ring.

8. Press `Enter` to save your changes.
9. Click `Next` until you find the **Button Assignments** area.

   If you want the user to have buttons on the telephone for do not disturb, go to cover, or send all calls, use the **Button Assignments** area to assign buttons. Note that you can use assign any, all, or none of the buttons, but you can make only one assignment per button.
10. Move to the button that you want to use and perform any of the following actions:
    - Type `dn-dst` after a button number if you want to assign a **do-not-disturb** button.
    - Type `goto-cover` after a button number if you want to assign a **go-to-over** button.
    - Type `send-calls` after a button number If you want to assign a **send-all-calls** button. When you click `Next` or press `Tab` or `Enter`, the system displays the **Ext** field. If you want to send calls to the extension you specified when you typed the `change station` command, leave the **Ext** field blank. If you want to send calls to another extension, type the extension number to which the system redirects calls when the user presses the send-calls button.
11. Press `Enter` to save your changes.

Related links

Creating a coverage path on page 368

Assigning a Consult button for a user

Procedure

1. Type `change station n`, where *n* is the extension of the user to whom you want to assign the Consult capability. Press `Enter`.
2. On the Station screen, click `Next` until you see the **Button Assignments** area.
3. In the **Button Assignments** area, type `consult` next to the button that you want the user to use for Consult.
4. Press `Enter` to save your changes.

Defining coverage redirected off-network calls

Procedure

1. Assign the telephone number for the external coverage point.
2. Administer the coverage path for calls redirected to external numbers.

Related links

Assigning the telephone numbers for the off-network coverage points on page 373
Administering the coverage path for redirected off-network calls on page 373

Preparing to define coverage for calls redirected off-net

Procedure

1. To view the Optional Features screen, Type `display system-parameters customer-options`. Press `Enter`.
2. Verify that the **Cvg of Calls Redirected Off-Net** field is set to y.

   If the **Cvg of Calls Redirected Off-Net** field is set to n, your system will not support the Call Coverage Off Network capability. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to coverage for calls redirected off-net, or to open a service request.

Assigning the telephone numbers for the off-network coverage points

Procedure

1. Type `change coverage remote` *n*, where *n* is the number of the Remote Call Coverage table that you want to change. Press `Enter`.

   Valid numbers are between 1 and 10.

   The system displays the Remote Call Coverage Table.
2. Type the telephone number (maximum of 16 digits) of the remote coverage point in one of the remote call coverage table fields.

   Note:

   If you need a digit to get outside your network, add the digit before the external number.

   The sequentially numbered fields in which you assign telephone numbers are called remote code numbers. You need this number to complete the procedure for defining coverage for calls redirected to external numbers.
3. Press `Enter` to save your changes.

Administering the coverage path for redirected off-network calls

Procedure

1. Type `change coverage path` *n*, where *n* is the number that is assigned to the coverage path that you want to administer for off-network coverage. Press `Enter`.

   The system displays the Coverage Path screen.

   Note:

   To enter an extension that is assigned as a vector directory number (VDN) as the last point in the coverage path, you must make an administration change. For more information, see the *Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780.
2. In the **Coverage Points** area, type the remote code number.

The **Point** field that you select determines where the number is used in the coverage path.

When you move to the next **Point** field the system displays the **Rng** field. If you want to use the number of rings displayed in the **Number of Rings** field on this screen, leave the **Rng** field blank.

If you do not want to use the number of rings displayed in the **Number of Rings** field on this screen, type the number of rings for this coverage point.

3. Press `Enter` to save your changes.

Assigning time-of-day coverage

Before you begin

You must Creating a coverage path before you can assign a time-of-day coverage path. To administer the coverage path, see Creating a coverage path.

Procedure

1. Set up a time-of-day coverage plan.
2. Assign a time-of-day coverage plan to a the extension of the user.

Related links

[Setting up a time-of day coverage plan](#) on page 374
[Assigning time-of-day coverage to a user](#) on page 375
[Creating a coverage path](#) on page 368

Setting up a time-of day coverage plan

Procedure

1. Enter `add coverage time-of-day next`.

   The system displays the next Time of Day Coverage Table screen. If this is the first Time of Day Coverage plan in your system, the table number is 1. This is the table number that you assign to a user extension.

```
                        TIME OF DAY COVERAGE TABLE: 1

          Act   Cvg      Act   Cvg      Act   Cvg      Act   Cvg      Act   Cvg
          Time  Path     Time  Path     Time  Path     Time  Path     Time  Path

Sun        0:00 3          :              :              :              :
Mon        0:00 3       08:00 1       17:30 2       20:00 3          :
Tue        0:00 3       08:00 1       17:30 2       20:00 3          :
Wed        0:00 3       08:00 1       17:30 2       20:00 3          :
Thu        0:00 3       08:00 1       17:30 2       20:00 3          :
Fri        0:00 3       08:00 1       17:30 2       20:00 3          :
Sat        0:00 3       08:00 1       17:30 2       20:00 3          :
```

2. To define your coverage plan, type the time period and the path number for each day of the week that you want to cover.

   Enter the time in a 24-hour format, from the earliest to the latest. For example, assume that coverage path 1 goes to the co-worker, coverage path 2 goes to the home, and coverage path 3 goes to voice mail. In this example, the user has the following coverage:

   - During the work day from 08:00 to 05:29, the system uses coverage path 1 to route calls to a co-worker.
   - In the evening from 05:30 to 19:59, the system uses coverage path 2 to route calls to home.
   - At night from 20:00 to 7:59 the following morning, the system uses coverage path 3 to route calls to voice mail.

     Define the path for the time period from 00:01 to 23:59 that you want coverage to operate. If you do not assign a coverage path to a specific time interval, no coverage exists from that time until the next coverage path activation time.

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

Assigning time-of-day coverage to a user

Procedure

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

   The system displays the Station screen.

2. In the **Coverage Path 1** field, type `t` plus the number of the Time of Day Coverage Table.
3. Press `Enter` to save your changes.

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.

Assigning Internal Alerting

Procedure

1. Type `change trunk-group n`, where *n* is the number of the trunk-group for which you want to administer Remote Access.
2. On the Trunk Group screen, click `Next` until you see the **Internal Alert** field.
3. In the **Internal Alert** field, perform one of the following actions:
   - If you want internal ringing and coverage for your system, type `y`.
   - If you do not want internal ringing and coverage for your system, type `n`.
4. Type `Enter` to save your changes.

Enabling enhanced Redirection Notification

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. On the Feature-Related System Parameters screen, click `Next` till you see the **Redirection Notification** field.
3. Enable notification for the features that you want by setting the respective **Display Notification for?** fields to `y`.
4. In the **Scroll Status messages Timer (sec.)** field, enter a value for the time delay between messages of different notification types.

   Leave the field blank to disable scrolling.

   For more information about the **Display Notification for** and **Scroll Status messages Timer** fields, see *Avaya Aura® Communication Manager Screen Reference*.
5. Press `Enter` to save your changes.

Reports for Call Coverage

The following reports provide information about the Call Coverage feature:

- The Coverage Path Measurement report shows coverage activity about the coverage paths.
- The Principal Coverage Measurement report shows coverage activity about the called extensions.
- The Call Detail Recording (CDR) report shows the outgoing trunk calls.

For detailed information on these reports and the associated commands, see *Avaya Aura® Communication Manager Reports*.

Considerations for Call Coverage

This section provides information about how the Call Coverage feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Coverage under all circumstances.

Tie-trunk calls

Incoming tie-trunk calls can be administered as either internal calls or external calls, and are redirected to Call Coverage accordingly.

Interactions for Call Coverage

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

Agent Call Handling

Do not assign Cover All Calls to agents who have the Automatic Answer option enabled. Any Automatic Call Distribution (ACD) or any non-ACD call to an extension on which Automatic Answer is enabled, and for which the coverage redirection criteria is administered as Cover All Calls, does not go to coverage. Instead, the call goes to the called extension. Cover All Calls redirection criteria do not affect incoming calls when a user is in the Auto-Answer mode.

Answer Detection

Coverage of Calls Redirected Off-Net (CCRON) competes with Answer Detection for call classifier ports.

Automatic Callback and Ringback Queuing

The system does not redirect callback calls to coverage. The caller can activate Automatic Callback when the user hears a ringing, redirection notification signal or a busy signal.

Automatic Intercom, Dial Intercom, and Priority Calling

The system does not redirect calls that use these features to coverage, unless the caller presses the **Go to Cover** button.

Attendant Vectoring and Tenant Partitioning

If a covered call does not route to an attendant in the first tenant group, you can route it to an attendant group of a different tenant partition. For example, you can reroute a call to Tenant Group B if the call is to cover to an attendant for Tenant Partition A but does not route to the attendant or is received out of hours when Attendant Group A is unstaffed.

To reroute the covered calls to another tenant attendant group, tenant attendant group B in this example,

1. In the vector for the tenant A attendant vectoring VDN, add a failure branch to a **route-to ldn_number with cov y if unconditionally** step for the LDN extension for the tenant group B.

2. The **With coverage** parameter of the route-to step must be set to **cov y** because the calls are covered otherwise it will not route to the VDN. Also the original coverage path, which covers to the tenant A attendant vectoring VDN, must have the **Cvg Enabled for VDN Route-to party?** field set to **y**.

Bridged Call Appearance

Coverage criteria for bridged call appearances are based entirely on the criteria of the primary extension that is associated with the bridged call appearance.

If a telephone user activates Send All Calls on the primary extension, incoming calls still ring bridged call appearances of that extension, as long as a simulated bridged appearance of the call is maintained at the primary extension.

While an off-network call is undergoing call classification, the system blocks a user from bridging onto the call.

Call Detail Recording (CDR)

When the **Coverage of Calls Redirected Off-Net** field (CCRON) is enabled, the system generates a CDR record only after the call is answered off the network. The dialed number in the record is the off-network number to which the call covers. The calling number is the station that is covered to the off-network destination.

Call Forwarding

Call Forwarding temporarily overrides the redirection criteria. When the redirection criteria are met at the forwarded-to extension, the system redirects the call to the coverage path of the forwarding extension.

The system supports calls that are forwarded off the network to be tracked for busy or no-answer conditions, and to return for further call-coverage processing under those conditions. However, if the called extension does not have a coverage path, the system does not track the call and the call is left at the off-network destination, regardless of whether the call is answered or busy.

For calls redirected to QSIG networks, if coverage after forwarding is disabled, the QSIG redirection takes precedence over the CCRON capability. However, if coverage after forwarding is enabled, CCRON takes precedence, enabling the call to be tracked back to the network to follow the coverage path.

If both Send All Calls and Call Forwarding are active, the system immediately redirects most calls to that extension to coverage. However, the system forwards priority calls to the designated forwarding destination.

If Cover All Calls is part of the coverage redirection criteria, and if Call Forwarding is active at an extension, the system immediately directs most calls to that extension to coverage. However, the system forwards priority calls to the designated forwarding destination.

In a call coverage criteria, if station A calls station B, station B has call coverage path assign to station C, and station C has Call forwarding enabled, call coverage in such scenario is unsuccessful.

Activation of Send All Calls at the forwarded-to extension does not affect calls that are forwarded to that extension.

Note:

If any coverage point has any flavor of call forward activated, then that coverage point will be skipped.

Call Pickup

Any call that the system directs to a covering user who is a member of a call pickup group can be answered by other members of the group.

Call Prompting

Coverage of Calls Redirected Off-Net (CCRON) competes with the Call Prompting feature for call classifier ports.

CallVisor ASAI

Coverage of Calls Redirected Off-Net (CCRON) competes with CallVisor for call classifier ports.

Centralized Attendant Service (CAS)

If an incoming CAS call is directed to a hunt group, the call is not redirected to the coverage path of the hunt group.

Class of Restriction (COR) and Controlled Restrictions

Users who might usually be restricted from receiving calls can receive calls that the system directs to them from the Call Coverage feature.

Conference

The system blocks users from conferencing another party onto a call that was routed off the network while the call is undergoing call classification. If any party on the call is on hold, the system routes the call off the network, but the system does not attempt to classify the call. The system routes the call off the network, even when the **Coverage of Calls Redirected Off-Net** field (CCRON) is enabled.

A call that covers to a vector directory number (VDN) cannot be added to a conference while the call is in vector processing.

Consult

If the covering party is talking to the principal after the covering party presses the **Consult** button, the covering party can use the Toggle Swap button to toggle back and forth between the caller and the principal.

Direct Department Calling (DDC), Uniform Call Distribution (UCD), and Automatic Call Distribution (ACD)

If a user with an **Auxiliary Work** button activates or deactivates Send All Calls, the Auxiliary Work function that is associated with the DDC feature or the UCD feature is activated or deactivated simultaneously.

If a user has no **Auxiliary Work** button, activating or deactivating Send All Calls makes the user unavailable or available, respectively, for DDC and UCD calls, but Auxiliary Work is not activated or deactivated. The user can use a Feature Access Code (FAC) to activate or deactivate Auxiliary Work mode.

Activating or deactivating the Auxiliary Work function does not activate or deactivate Send All Calls.

Direct Outward Dialing (DOD)

Coverage of Calls Redirected Off-Net (CCRON) competes with DOD for call classifier ports when DOD uses MFC signaling. The Call Classifier - Detector port provides the MFC tones. Non-MFC DOD calls do not need the Call Classifier - Detector port for this purpose, because Non-MFC DOD calls do not need MFC tones.

Global Call Classification

To classify tones in countries that do not use the USA tone plan, time cadences and frequencies must be administered so that time cadences and frequencies can be downloaded to the G4xx Media Gateway.

Hold

If a covering user puts a call on hold, and the called user picks up on the call, the coverage appearance might be dropped, depending on administration.

If any party is on hold when the system routes a coverage call off the network, that call does not undergo call classification. In this case, the call does not undergo call classification, even when the **Coverage of Calls Redirected Off-Net** (CCRON) field is enabled on your system.

Internal Automatic Answer (IAA)

If call coverage redirection criteria redirects an internal call to another telephone, that call is eligible for IAA at that telephone.

IAA does not apply to calls to the original called extension when the:

- User at the called extension has Do Not Disturb, Send All Calls, or Cover All Calls active
- Calling user selects Go To Cover before the user places the call

  Calls that are directed to a Coverage Answering Group cannot use IAA.

ISDN End-to-End Calls

When ISDN facilities carry an off-network coverage call end-to-end, call classification is accomplished through the ISDN protocol, rather than by a call classifier port.

Leave Word Calling (LWC)

Call Coverage can be used with or without LWC. However, the two features complement each other. When a covering user activates LWC during a coverage call, a message is left for the called user to call the covering user. When a covering user activates Coverage Callback during a coverage call, a message is left for the called user to call the internal caller.

Tenant Partitioning

The Tenant Partitioning feature might not block coverage calls across tenant partitions.

Interaction for Enhanced Redirection Notification

The following are the interactions for the enhanced Redirection Notification:

Bridged Call Appearance

Does not work on stations that have no call appearance of their own.

Call Forwarding

Applies to Call Forwarding All, Call Forwarding Busy/Don’t Answer, and Enhanced Call Forwarding.

Do Not Disturb

Applies to Do Not Disturb whether activated from the station or from an attendant console.

Call Coverage Troubleshooting

This section lists the known or common problems that users might experience with the Call Coverage feature:

Problem	Possible cause	Action
The system redirects some unanswered calls to the Attendant console, instead of the coverage path.	A call that is transferred internally, and unanswered within the interval that is specified in the Return Call Timeout of the Console Parameters screen, redirects to the attendant console.	Verify that the called extension has a coverage path by typing the **`status station`** command. If the **active coverage option** field on the Station screen has a coverage path, increase the number of seconds in the Return Call Timeout interval on the Console Parameters screen. Increase the interval so that it exceeds the total time that a call rings on the called extension and all points in the coverage path of the called extension.
The system does not redirect to the correct destination in the coverage path of the called extension.	The called extension is forwarded to another destination.	Type the **`status station`** command to determine if either Call Forwarding or Send All Calls is active at the called extension. If the **CF Destination Ext** field contains a forwarded-to extension, cancel Call Forwarding for the called extension. If the **SAC Activated?** field is set to yes, cancel Send All Calls for the called extension.
	The coverage path that you assigned to the called extension is incorrect.	Type the **`display station`** command to verify that you assigned the correct coverage path to the called extension. Change the coverage path if the coverage path is not the coverage path that you want for the called extension.

Table continues…

Problem	Possible cause	Action
The system does not redirect to the coverage path of the called extension.	The points in the coverage path are unavailable.	Run the **`status station`** command to determine if either Call Forwarding or Send All Calls is active at the called extension. If the **CF Destination Ext** field contains a forwarded-to extension, cancel Call Forwarding for the called extension. If the **SAC Activated?** field is set to yes, cancel Send All Calls for the called extension. If the coverage path of the called extension contains a hunt group, ensure that the length of the queue is sufficient to contain all the calls that the system redirects to the hunt group.

Limitations of Call Coverage

Scenario	Condition	Result
A 5-party conference call is in progress and a 12-party-conference is set to N, and maintain temporary bridge appearance on pick-up is set to Y	Then, if a caller calls a user and the call is picked up by pick up group member, and the caller tries to conference these two calls	The conference is denied.
An 11-party conference call is in progress and a 12-party-conference is set to Y, and maintain temporary bridge appearance on pick-up is set to Y	Then, if a caller calls a user and the call is picked up by pick up group member, and the caller tries to conference these two calls	The conference is denied.
A 5-party conference call is in progress and a 12-party-conference is set to N, and maintain simulated bridge appearance on principal on pick-up is set to Y on system-paramter-coverage-forwarding screen	Then, if a caller calls a user and the call is answered by coverage point, and the caller tries to conference these two calls	The conference is denied.

Table continues…

Scenario	Condition	Result
An 11-party conference call is in progress and a 12-party-conference is set to Y, and maintain simulated bridge appearance on principal on pick-up is set to Y on system-paramter-coverage-forwarding screen	Then, if a caller calls a user and the call is answered by coverage point, and the caller tries to conference these two calls	The conference is denied.

Chapter 54: Call Detail Recording

Use the Call Detail Recording (CDR) feature to record information on incoming, outgoing, and tandem calls for each trunk group that you administer for CDR, including auxiliary trunks. The system records information on each trunk-group call and each station-to-station call.

Detailed description of Call Detail Recording

Use the Call Detail Recording (CDR) feature to record information on incoming, outgoing, and tandem calls for each trunk group that you administer for CDR, including auxiliary trunks. The system records information on each trunk-group call and each station-to-station call.

You can also request that CDR record information on:

- Temporary signaling connections (TSCs) that involve trunks
- Calls that use loudspeaker paging
- Calls to which account code dialing or a Feature Access Code (FAC) apply
- Ineffective call attempts

  If you request that the system record information about ineffective call attempts, you increase the number of calls that the system records. However, the request to record ineffective call attempts can also help you to increase security, because the system records call attempts that are blocked because of insufficient calling privileges.

  Information on ineffective call attempts can also show you that your users cannot make calls because all the trunks on your system are busy.
- The audio service link calls that the switch uses for IP softphones that are set up as telecommuter IP softphones.

  An IP softphone can use one audio service link to make many short calls. The system shows these many short calls as one long call on the CDR reports.

Some call accounting systems do not support all the information that CDR offers. See your Avaya representative for information on how CDR operates on your system.

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 CDR data format - TELESEER for Communication Manager 4.0 or later on page 401 through CDR data format - int-ISDN for Communication Manager 4.0 or later on page 418).

Monitoring call detail records

You can monitor call detail records daily for unusual calling patterns, long calls, international calls, calls that are outside the normal business hours, and other indications of toll fraud. Call accounting systems are available that automatically monitor CDR output for fraudulent calling patterns.

Legacy CDR and Survivable CDR

Beginning with Communication Manager Release 5.0, you can have Legacy or Conventional CDR or Survivable CDR for your system. Both methods provide the identical call accounting information and support the same CDR formats.

In a Legacy CDR environment, Communication Manager generates all CDR records on the active server and then exports the records to a CDR adjunct (using IP links) for further processing. In these systems, the CDR adjunct functions in a “listen only” mode receiving the records sent by Communication Manager. This type of CDR processing was used exclusively in Communication Manager up through Release 3.X. In a Legacy CDR environment, the system cannot collect CDR records when link between the main, Survivable Remote Server and/or Survivable Core Server and CDR adjunct is down (this is generally the case when a Survivable Remote Server or Survivable Core Server is active). It also requires the IP link between Communication Manager and the CDR adjunct to be up at all times.

Communication Manager 4.x or later introduced a new method of data collection called Survivable CDR. Survivable CDR stores CDR data records on the Communication Manager server’s local hard drive, if required. The CDR adjunct then periodically polls each the Communication Manager server and collects the CDR data files from the servers. Survivable CDR was introduced in Communication Manager Release 4.0 and it was only supported on Survivable Remote Server platforms. Beginning with Communication Manager Release 5.0, Survivable CDR is supported on all Communication Manager platforms, that is, on the “mains”, Survivable Remote Server and Survivable Core Server. Survivable CDR transfers CDR data in an encrypted manner from the Communication Manager server to the CDR adjunct using the Secure File Transfer Protocol (SFTP). Note that Survivable CDR requires updated CDR adjuncts. CDR records are stored and transferred in batches, rather than one record at a time as with Legacy CDR.

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.

Related links

File naming conventions for Survivable CDR on page 387

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`.

QSIG Supplementary Service - Advice of Charge

Beginning with Communication Manager Release 4.0 or later, 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.

The following describes a call flow with the QSIG Supplementary Service - Advice of Charge feature:

1. A user places a call through the private telecommunication network (PTN) and into the public switching telecommunication network (PSTN).
2. Charging information from the PSTN is conveyed to the gateway switch either:
   - At intervals during the call and at the end of the call, or
   - Only at the end of the call

   This is determined by Communication Manager administration, and by subscription, at the gateway switch, of Charge Advice with the PSTN Service Provider.
3. If Communication Manager is the gateway, CDR information may be recorded at the gateway and routed to the user's switch for recording there as well. This enables accounting the call to an end user in addition to recording the trunk used.
4. If there is a tandem node in the call path, the tandem node may also send call record data to a CDR port.
   - If the tandem node is a Tenovis I55, the record can contain charge information.
   - If the tandem node is Communication Manager, the record is passed without Communication Manager doing anything with it.

Customer options that are required for the feature are ISDN, QSIG Basic Call and QSIG Basic Supplementary Services. These options are typically activated by enabling the Communication Manager - Enterprise Edition RFA file.

To use this feature, you must have adjunct devices that are capable of logging or interpreting CDR output formats that record ISDN Call Charge.

Existing PRI, BRI, and H.323 hardware interfaces providing QSIG and bearer transport are used for this feature.

Administering Charge Advice for QSIG trunks

Procedure

1. On the Trunk Group screen, click `Next` until you see the **Charge Advice** field.
2. Enter `during-on-request`, `end-on request`, or `none`

   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. Click `Next` until you see the **Decimal Point** field.
4. Enter `comma`, or `period`.

   Note:

   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.

Answer Detection for CDR

Communication Manager provides three methods to determine whether the called party answers a call:

- Call classification
- Network answer supervision
- Answer supervision by timeout

Call classification for CDR

A call-classifier media module detects tones and voice-frequency signals on the line to determine whether a call is answered. This method is accurate. The calls that are answered are classified correctly. The following exceptions exist:

- Miscellaneous tones, such as confirmation tones, might be classified as answers.
- Loud background noise might activate answer detection, and cause a call to be classified as answered, even if the call is not connected.

- Some calls that are answered might be incorrectly classified as fast busy signals.
- Call classifier media module packs do not recognize Special Information Tones (SIT) as answers.

The system generates a call record for any call that is classified as answered, whether the classification is correct or incorrect. If Call Classification incorrectly classifies a call as answered, and the call is subsequently answered, the call duration that CDR reports includes both the time between the incorrect classification and the actual answer, and the remaining duration of the call.

Network answer supervision for CDR

The central office (CO) sends a signal to the originating switch when the far end answers a call. If a call travels over a private network before the call reaches the CO, the signal is transmitted back over the private network to the originating switch. This method is extremely accurate, but network answer supervision is unavailable over most loop-start trunks. For example, network answer supervision is unavailable over CO, foreign exchange (FX), and Wide Area Telecommunications Service (WATS) trunks in the US.

Answer supervision by timeout for CDR

If the caller is off-hook when the answer timer expires, the system assumes that the outgoing call is answered. Answer supervision by timeout is the least accurate method to detect that a call is answered. Calls that are shorter than the timer duration do not generate call records. Calls that ring for a long time produce call records, even if the calls are unanswered.

Network answer supervision overrides answer supervision by timeout.

Account Code Dialing for CDR

Use the Account Code Dialing capability to associate a call with an account number. A user enters a FAC for Account Code Dialing before a user dials a telephone number. You can specify that the use of the FAC is mandatory or optional for the user. When a user dials a telephone number and the FAC, the system records the:

- Telephone number
- Account code
- Trunk Access Code (TAC), or the Automatic Route Selection (ARS) access code

The system does not record the FAC for Account Code Dialing.

Forced Entry of Account Codes for CDR

If you require that users enter an account code FAC, you have several options. You can require that:

- All users enter an account code for all calls
- All users enter an account code for calls that are made on a specific trunk.
- All users enter an account code for calls that are made to a specific telephone number

- A specific user enters an account for all calls that are made by that user

If you use the Forced Entry of Account Codes (FEAC) capability, the system rejects any call that a user makes without an account code FAC, if the call requires an account code. When the system rejects the call, the user hears intercept tone.

Avaya recommends that you use the FEAC capability to make your system more secure.

Note:

The system does not verify account codes. The system only verifies that the user enters the number of digits that you specify. If you want the system to verify account codes, you need to use the Authorization Codes feature. For more information, see the “Authorization Codes” feature.

The following types of calls never require an account code:

- Calls that an attendant makes
- Calls that an attendant makes to determine if a trunk is busy
- Calls that a user makes to determine if a trunk is busy
- Distributed Communications System (DCS) calls, unless the Class of Restriction (COR) of the trunk requires an account code
- Personal Central Office Line (PCOL) calls
- Remote access calls that do not have barrier codes
- Trunk-to-trunk calls

Call Splitting for CDR

You use the Call Splitting capability to record information about the following calls that:

- Are part of a conference
- Transferred
- Involve an attendant

The system records a separate CDR record for each participant on any of these types of calls.

You can request call splitting information for both incoming and outgoing trunks. You can also request call splitting information for an attendant call on an incoming trunk, and for an attendant call on an outgoing trunk

Incoming trunk call splitting for CDR

If you request incoming trunk call splitting (ITCS) information for a call, the system creates a CDR record when a user uses the Conference feature or the Transfer feature. The CDR record includes the:

- Duration of the user participation
- Incoming TAC

- Number that the caller dialed
- Condition code

When a user drops a call, or successfully transfers a call, the system records the action of the user. The duration of a transferred call starts when the transferring party presses the transfer button for the second time.

When a user uses the Conference feature for an incoming trunk call, the system creates a CDR record when the user adds a participant to the conference call. The CDR record of these calls shows the duration of the call for each user who participated. The CDR records of a conference call contain duration information that overlaps.

The system creates an incoming trunk call record when:

- A user requests ITCS for the system.
- A user adds another user to a conference call, or transfers a call to another user.
- The user who is added to the conference call, or who is transferred, is on a local extension that has the Intraswitch CDR option activated.

The system does not create an Intraswitch CDR record.

Examples of incoming trunk call splitting

ITCS and a conference call example

The following example shows the interaction between the participants of a conference call and the system, when ITCS is active, and all participants are on the same server:

- Caller A, at extension 123, makes an incoming trunk call to participant B, at extension 565-7890.
- Caller A and participant B talk for 2 minutes.
- Participant B adds participant C, at extension 5-4321, to the conference call.
- Participant B adds participant D, at extension 5-9876, to the conference call.
- Caller A, participant B, participant C, and participant D talk for an additional 8 minutes.
- Participant B drops the call.
- The system creates a CDR record for call segment A-B.
- Caller A, participant C, and participant D talk for an additional 5 minutes.
- Caller A, participant C, and participant D drop the call.
- The system creates two additional CDR records, one for call segment A-C and one for call segment A to D. Note that each CDR record shows the incoming trunk ID as the calling number, 123.

ITCS conference call on the same server on page 393 shows the CDR information that changes when ITCS is active during a conference call. The call durations are approximate.

Table 12: ITCS conference call on the same server

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
A-B	0:10:0	C	-	123	5657890
A-C	0:13:0	C	-	123	54321
A-D	0:13:0	C	-	123	59876

ITCS and a call transfer on the same server example

The following example shows the interaction between the participants of a transfer call and the system when ITCS is active, and all participants are on the same server:

- Caller A, at extension 123, calls participant B, at extension 565-7890.
- Caller A and participant B talk for 1 minute.
- Participant B transfers the call to participant C, at extension 5-4321.
- The system creates a CDR record for call segment A-B.
- Caller A and participant C talk for an additional 5 minutes.
- Caller A and participant C drop the call.
- The system creates a CDR record for call segment A-C.

ITCS transfer on the same server on page 393 shows the CDR information this scenario. The call durations are approximate.

Table 13: ITCS transfer on the same server

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
A-B	0:01:0	9	-	123	5657890
A-C	0:05:0	9	-	123	54321

ITCS and a call transfer to the public network example

The following example shows the interaction between the participants of a transfer call and the system when ITCS is active, and all the participants are not on the same server:

- Caller A, at extension 123 on server, calls participant B, at extension 565-7890.

  Both caller A and participant B are on the same server.
- Caller A and participant B talk for 1 minute.
- Participant B transfers the call to participant C, at telephone number 566-5555.

  Participant C is on the public network.
- Participant A and participant C talk for an additional 4 minutes.

- Participant A and participant C drop the call.
- The system creates two CDR records, one for call segment A-B, and one for call segment A-C.

ITCS transfer to an outgoing trunk on page 394 shows the CDR information that changes when ITCS is active during a call transfer. The call durations are approximate. Note that the duration of the original incoming trunk call, call segment A to B, includes the duration of the conversation between caller A and participant B, and the duration of the conversation between participant B and participant C.

Table 14: ITCS transfer to an outgoing trunk

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
A-B	0:01:0	9	-	123	5657890
A-C	0:04:0	9	345	123	5665555

Outgoing trunk call splitting for CDR

If you request outgoing trunk call splitting (OTCS), the system creates CDR records of transferred outgoing calls in the same manner as for ITCS. See ITCS and a call transfer on the same server on page 393 and ITCS and a call transfer to the public network on page 394 for a description of the CDR information on transfer calls when ITCS is active.

If a user requests OTCS and originates a conference call, the call duration for that user starts when the user originates the call. The call duration for that user ends when the user drops the call. When that user drops the call, the system creates a second CDR record for the users who remain on the conference call.

Examples of outgoing trunk call splitting

OTCS and a conference call on the public network example

The following example shows the interaction between the participants of a transfer call and the system, when OTCS is active, and all the participants are not on the same server:

- Caller A, at extension 123 on server, calls participant B, at telephone number 777-7890.

  Participant B is on the public network.
- Caller A and participant B talk for 5 minutes
- Caller A adds participant C to the conference call.
- Participant B transfers the call to participant C, at telephone number 777-5678.

  Participant C is on the public network.
- Caller A, participant B, and participant C talk for an additional 5 minutes.
- Caller A, participant B, and participant C drop the call.

- The system creates two CDR records, one for call segment A-B, and one for call segment A-C.

OTCS conference call on page 395 shows the CDR information that changes when OTCS is active during a conference call. The call durations are approximate.

Table 15: OTCS conference call

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
A-B	0:10:0	C	345	57890	7771234
A-C	0:05:0	C	345	57890	7775678

OTCS and a call transfer to the public network example

The following example shows the interaction between the participants of a transfer call and the system when OTCS is active, and all the participants are not on the same server:

- Caller A, at extension 51234 on server, calls participant B, at telephone number 777-7890.

  Participant B is on the public network.
- Caller A and participant B talk for 5 minutes.
- Caller A transfers the call to participant C at extension 54444.

  Caller A and participant C are on the same server.
- The system creates two CDR records, one for call segment A-B and one for call segment C-B.

OTCS call transfer on page 395 shows the CDR information that changes when OTCS is active during a call transfer. The call durations are approximate.

Table 16: OTCS call transfer

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
A-B	0:05:0	A	345	51234	7777890
C-B	0:05:0	A	345	54444	7777890

ITCS, OTCS, and attendant call recording for CDR

If you request either ITCS or OTCS, you have the option for the system to generate a CDR record of the attendant portion for calls that are transferred.

If you request either ITCS or OTCS, the system always creates a separate CDR record of the attendant portion of a conference call.

Examples of ITCS, OTCS, and attendant call recording

ITCS or OTCS and an attendant incoming trunk call transfer example

The following example shows the interaction between the participants of a transfer call and the system, when either ITCS or OTCS is active:

- Caller A, at TAC 123, calls the attendant, and asks the attendant to transfer the call to participant B, at extension 5-888

  Caller A is on the public network.

  The attendant and participant B are on the same server.
- Caller A and the attendant talk for 1 minute.
- Caller A and participant B, talk for 5 minutes.
- The system creates two CDR records, one for call segment A-Attd, and one for call segment A-B.

Attendant transfer of an incoming trunk call on page 396 shows the CDR information that changes when ITCS or OTCS is active when an attendant transfers an incoming public network call.

Table 17: Attendant transfer of an incoming trunk call

Call Segment	Call Duration	Condition code	Access code used	Calling number	Dialed number
A-Attd	0:01:0	9	-	123	Attd
A-B	0:05:0	9	-	123	58888

ITCS or OTCS and an attendant call transfer on a public network trunk example

The following example shows the interaction between the participants of a transfer call and the system, when either ITCS or OTCS is active, and an attendant transfers a call to the public network:

- The attendant dials participant A at extension 5-9999.
- The attendant and participant A talk for 1 minute.
- The attendant transfers the call to participant B at telephone number 444-5678.
- The participant A and participant B talk for 5 minutes.
- The system creates two CDR records, one for call segment A-Attd, and one for call segment A-B.

Attendant call transfer on a public network trunk on page 397 shows the CDR information that changes when ITCS or OTCS is active when an attendant transfers a call to an outgoing public network trunk.

Table 18: Attendant call transfer on a public network trunk

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
Attd-A	0:01:0	A	345	Attd	59999
A-B	0:05:0	A	345	59999	4445678

Intraswitch CDR

The system uses the Intraswitch CDR capability to create CDR records for calls to and from users on the same local server. Before the system can create an intraswitch CDR record, you must assign the Intraswitch CDR capability for one of the extensions.

If you enable ITCS for your system, and you assign the Intraswitch CDR capability for an extension, the system-wide ITCS overrides the Intraswitch CDR for the extension. When the system-wide ITCS overrides the Intraswitch CDR for the extension, the system generates trunk call records for an incoming trunk call to the extension. The system does not generate Intraswitch CDR records for an incoming trunk call to the extension.

The records that the system creates for the Intraswitch CDR capability are similar to the records that the system creates for other CDR records. However, some of the information differs. For example, the system does not provide TACs or circuit IDs for intraswitch calls, because that information is unnecessary.

Some calls might appear to be intraswitch CDR calls, but are actually trunk calls. For example, the system creates a trunk CDR record for an internal call to an extension that is forwarded to an outgoing trunk, even if you assigned the Intraswitch CDR capability for either station.

You can assign the Intraswitch CDR capability to:

- A Terminating Extension Group (TEG)
- A station
- A data module
- A Vector Directory Number (VDN)
- A Primary Rate Interface (PRI)
- An endpoint
- An access endpoint
- A hunt group

The number in the **Dialed Number** field depends on whether you administered the CDR System Parameters to record hunt group/member or VDN information. You cannot assign the Intraswitch CDR capability to an attendant console or a CallVisor Adjunct-Switch Application Interface (ASAI) station.

Note that the system generates a CDR record for a call only if the user is the caller or the recipient of the call, and has the Intraswitch CDR capability active for the extension of the user. For example, if the user participates in the call as the result of Call Pickup or Call Forwarding, the system does not create a CDR record.

CDR Privacy

Use the CDR Privacy capability to maintain the privacy of the caller. The system replaces some of the digits that the user dials with blanks. The system records the call information, including the account number that the user enters. But the CDR information does not show the telephone number that the user dials.

You can assign the CDR Privacy capability individually to each of your users. You decide the number of digits that the system replaces with blanks. The system then uses this information for all calls of the users to whom you assign the CDR Privacy capability.

The CDR Privacy capability does not apply under the following conditions:

- Some countries require that the system replace a specific number of the digits that the user dials with blanks. If a country requires that the system replace a specific number of the digits that the user dials with blanks, the requirement applies to all calls.
- When an adjunct-originated call is made on behalf of a hunt group, and the **Calls to Hunt Group - Record** field on the CDR System Parameter screen is set to group-ext, CDR Privacy does not apply. However, CDR Privacy does apply if the **Hunt Group - Record** field is set to member extension.
- When an adjunct-originated call is made on behalf of a hunt group and the **Calls to Hunt Group - Record** field on the CDR System Parameter screen is set to member-ext, then CDR Privacy applies.
- Some report processors do not support the CDR Privacy capability.

CDR output port formats

When operating in Legacy CDR mode, you can administer two CDR output ports, the Primary and the Secondary. You can administer different CDR formats for each of these two output ports. The Secondary port is generally used to troubleshoot network issues, or view CDR records locally.

CDR record formats

Communication Manager 4.0 and later provides a new field **Use Legacy CDR Formats?** on the CDR System Parameters screen for the system administrator to choose either the Communication Manager 3.x (legacy) CDR formats, or the new Communication Manager formats to create CDR records for the system.

The default value for this field is y which uses the legacy formats.

When the **Use Legacy CDR Formats** field is set to n, the system uses the new Communication Manager formats. The **INS** field in the CDR records increases from three to five characters and the **Attendant Console** field increases from two characters to four characters.

Note:

For information on CDR formats for Communication Manager 4.0 or later, see CDR data format - TELESEER for Communication Manager 4.0 or later on page 401 through CDR data format - int-ISDN for Communication Manager 4.0 or later on page 418 of this

document. For more information on legacy CDR formats, see CDR data format - TELESEER for Communication Manager 3.x on page 420 through CDR data format - int-ISDN for Communication Manager 3.x on page 437.

Note:

The CDR record tables that changed for Communication Manager 4.0 or later are CDR data format - ISDN TELESEER for Communication Manager 4.0 or later on page 402, CDR data format - enhanced printer for Communication Manager 4.0 or later on page 406, Pull Transfer on page 1366, CDR data format - enhanced LSU for Communication Manager 4.0 or later on page 410, CDR data format - expanded for Communication Manager 4.0 or later on page 410, CDR data format - enhanced expanded for Communication Manager 4.0 or later on page 412, CDR data format - unformatted for Communication Manager 4.0 or later on page 414, CDR data format - enhanced unformatted for Communication Manager 4.0 or later on page 415, and CDR data format - int-ISDN for Communication Manager 4.0 or later on page 418. All other CDR record tables remain unchanged between Communication Manager 4.0 and prior releases.

For more information, see *Avaya Aura® Communication Manager Screen Reference*.

The system sends two types of records to the CDR output device, a date record and a call detail record.

CDR date record format

CDR sends date information to the CDR device once a day at midnight, or when someone connects the device to the system. The record that the system generates at this time is a noncall record, and contains only the information that is shown in one of the date record formats.

Three date record formats exist:

- CDRU
- Printer
- TELESEER

The records that the system sends to the TELESEER and the printer contain the date only. The records to the CDRU contain time. These tables are the same for “legacy” and Communication Manager 4.0 or later.

- Date record format to LSU, LSU-expand, unformatted, and customized on page 400
- CDR date record format for printer and expanded on page 400
- CDR date record format for TELESEER 59 character, int-proc, int-direct, and int-ISDN on page 400

Date record format to LSU, LSU-expand, unformatted, and customized

Table 19: Date record format to LSU, LSU-expand, unformatted, and customized

Position	Description
1-2	Hour (leading 0 added if needed)
3	Colon (:)
4-5	Minute (leading 0 added if needed)
6	Blank
7-8	Month (leading 0 added if needed)
9	Slash (/)
10-11	Day (leading 0 added if needed)
12	Carriage return
13	Line feed
14-16	Null

CDR date record format for printer and expanded

Table 20: Date record format for printer and expanded

Position	Data field description
1-2	Month (leading 0 added if needed)
3	Space
4-5	Day (leading 0 added if needed)
6	Carriage return
7	Line feed
8-10	Null

CDR date record format for TELESEER 59 character, int-proc, int-direct, and int-ISDN

Table 21: Date record format for TELESEER 59 character, int-proc, int-direct, and int-ISDN

Position	Data field description
1-2	Month (leading 0 added if needed)
3-4	Day
5	Carriage return
6	Line feed
7-9	Null

Customized CDR call record formats

You can use the customized record formats to define the call records for your system. You can determine the data elements that you want, and the position of the data elements in the record.

However, the device that you use to interpret the CDR data must be programmed to accept the data formats that you choose. Consult your Avaya representative before you use a customized record format.

Standard CDR call record formats for Communication Manager 4.0 or later

See the following tables for a description of the standard call record formats for Communication Manager 4.0 or later.

CDR data format - TELESEER for Communication Manager 4.0 or later

Table 22: CDR data format - TELESEER for Communication Manager 4.0 or later

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes
11	Duration-tenths of minutes
12	Condition code
13-15	Access code dialed
16-18	Access code used
19-33	Dialed number
34-38	Calling number
39-53	Account code
54	facilities restriction level (FRL)
55	inter-exchange carrier (IXC)
56-58	Incoming circuit ID
59-61	Outgoing circuit ID
62	Feature flag
63-69	Authorization code
70-76	Space
77	Carriage return
78	Line feed
79-81	Null

CDR data format - ISDN TELESEER for Communication Manager 4.0 or later

Table 23: CDR data format - ISDN TELESEER for Communication Manager 4.0 or later

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes
11	Duration-tenths of minutes
12	Condition code
13-15	IXC
16-18	Access code used
19-33	Dialed number
34-38	Calling number
39-53	Account code
54	INS (units)
55	FRL
56-58	Incoming circuit ID
59-61	Outgoing circuit ID
62	Feature flag
63-69	Authorization code
70-73	INS (ten-thousands, thousands, hundreds, tens)
74-78	Space
79	Line feed
80-82	Null

CDR data format - enhanced TELESEER for Communication Manager 4.0 or later

Table 24: CDR data format - enhanced TELESEER for Communication Manager 4.0 or later

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes

Table continues…

Position	Description
11	Duration-tenths of minutes
12	Condition code
13-16	IXC code
17-19	Access code used
20-34	Dialed number
35-39	Calling number
40-54	Account code
55	ISDN NSV (units)
56	FRL
57-59	Incoming circuit ID
60-62	Outgoing circuit ID
63	Feature flag
64-70	Authorization code
71-74	ISDN NSV (ten-thousands, thousands, hundreds, tens)
75-78	Space
79	Carriage return
80	Line feed
81-83	Null

CDR data format - 59 character for Communication Manager 4.0 or later

Table 25: CDR data format - 59 character for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-12	Access code dialed
13-15	Access code used
16-30	Dialed number
31-35	Calling number
36-50	Account code
51	FRL

Table continues…

Position	Description
52	IXC
53-55	Incoming circuit ID
56-58	Outgoing circuit ID
59	Carriage return
60	Line feed
61-63	Null

CDR data format - printer for Communication Manager 4.0 or later

Table 26: CDR data format - printer for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	Access code dialed
16	Space
17-19	Access code used
20	Space
21-35	Dialed number
36	Space
37-41	Calling number
42	Space
43-57	Account code
58	Space
59-65	Authorization code
66-69	Space
70	FRL
71	Space
72	IXC

Table continues…

Position	Description
73	Space
74-76	Incoming circuit ID
77	Space
78-80	Outgoing Circuit ID
81	Space
82	Feature flag
83	Carriage return
84	Line feed

CDR data format - ISDN printer for Communication Manager 4.0 or later

Table 27: CDR data format - ISDN printer for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	IXC
16	Space
17-19	Access code used
20	Space
21-35	Dialed number
36	Space
37-41	Calling number
42	Space
43-57	Account code
58	Space
59-65	Authorization code
66	Space
67-70	INS (ten thousands thousands, hundreds, tens)

Table continues…

Position	Description
71	Space
72	INS (units)
73	Space
74	FRL
75	Space
76-78	Incoming circuit ID
79	Space
80-82	Outgoing circuit ID
83	Space
84	Feature flag
85	Carriage return
86	Line feed

CDR data format - enhanced printer for Communication Manager 4.0 or later

Table 28: CDR data format - enhanced printer for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	IXC code
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-43	Calling number
44	Space
45-59	Account code

Table continues…

Position	Description
60	Space
61-67	Authorization code
68	Space
69-73	ISDN NSV
74	Space
75	FRL
76	Space
77-79	Incoming circuit ID
80	Space
81-83	Outgoing Circuit ID
84	Space
85	Feature flag
86	Carriage return
87	Line feed

CDR data format - LSU-expand for Communication Manager 4.0 or later

Table 29: CDR data format - LSU-expand for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	Access code dialed
16-18	Access code used
19	Space
20-34	Dialed number
35	Space
36-39	Calling number
40	Space

Table continues…

Position	Description
41-45	Account code
46	Space
47-53	Authorization code
54-57	Space
58	FRL
59	Space
60	Calling number (1st digit)
61	Space
62-63	Incoming circuit ID (tens, units)
64	Space
65	Feature flag
66	Space
67-68	Outgoing circuit ID (tens, units)
69	Space
70	Outgoing circuit ID (hundreds)
71	Space
72	Incoming circuit ID (hundreds)
73	IXC
74	Carriage return
75	Line feed
76-78	Null

CDR data format - LSU for Communication Manager 4.0 or later

Table 30: CDR data format - LSU for Communication Manager 4.0 or later

Position	Description
1	Duration-hours
2-3	Duration-minutes
4	Duration-tenths of minutes
5	Condition code
6-8	Access code dialed
9-11	Access code used
12-26	Dialed number
27-30	Calling number (digits 2-5 for a 5-digit dial plan)
31-35	Account code (first 5 digits)

Table continues…

Position	Description
36-42	Authorization code or digits 6-12 of the account code
43-44	Space or digits 13-14 of account code
45	FRL or digit 15 of the account code
46	Calling number (1st digit)
47-48	Incoming circuit ID (tens, units)
49	Feature flag
50-52	Outgoing circuit ID (tens, units, hundreds)
53	Incoming circuit ID (hundreds)
54	IXC
55	Carriage return
56	Line feed
57-59	Null

CDR data format - ISDN LSU for Communication Manager 4.0 or later

Table 31: CDR data format - ISDN LSU for Communication Manager 4.0 or later

Position	Description
1	Duration-hours
2-3	Duration-minutes
4	Duration-tenths of minutes
5	Condition code
6-8	IXC
9-11	Access code used
12-26	Dialed number
27-30	Calling number (digits 2-5 for a 5-digit dial plan)
31-35	Account code (digits 1-5)
36-42	Authorization code or digits 6-12 of the account code
43-45	INS (ten thousands, thousands, hundreds, or digits 13-14 of account code
46-47	INS (tens, units), FRL, or digit 15 of the account code
48	Calling number (1st digit of a 5-digit calling number)
49-50	Incoming circuit ID (tens, units)
51	Feature flag
52-54	Outgoing circuit ID (tens, units, hundreds)
55	Incoming circuit ID (hundreds)
56	FRL

Table continues…

Position	Description
57	Carriage return
58	Line feed
57-61	Null

CDR data format - enhanced LSU for Communication Manager 4.0 or later

Table 32: CDR data format - enhanced LSU for Communication Manager 4.0 or later

Position	Description
1	Duration-hours
2-3	Duration-minutes
4	Duration-tenths of minutes
5	Condition code
6-9	IXC code
10-12	Access code used
13-27	Dialed number
28-31	Calling number
32-35	Account code (digits 1-4)
36-42	Authorization code or digits 6-12 of the account code
43-47	ISDN NSV
48	1st digit of a 5-digit calling number
49-50	Incoming circuit ID (tens, units)
51	Feature flag
52-54	Outgoing circuit ID (tens, units, hundreds)
55	Incoming circuit ID (hundreds)
56	FRL
57	Carriage return
58	Line feed
59-61	Null

CDR data format - expanded for Communication Manager 4.0 or later

Table 33: CDR data format - expanded for Communication Manager 4.0 or later

Position	Description
1-2, 3-4	Time of day-hours, -minutes
5	Space

Table continues…

Position	Description
6, 7-8, 9	Duration-hours, minutes, tenths of minute
10	Space
11	Condition code
12	Space
13-16	Access code dialed
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number
49	Space
50-64	Account code
65	Space
66-72	Authorization code
73-76	Space
77	FRL
78	Space
79-81	Incoming circuit ID
82	Space
83-85	Outgoing circuit ID
86	Space
87	Feature flag
88	Space
89-92	Attendant console
93	Space
94-97	Incoming trunk access code
98	Space
99-100	Node number
101	Space
102-106	INS
107	Space
108-110	IXC
111	Space
112	Bearer capability class (BCC)

Table continues…

Position	Description
113	Space
114	Message-Associated User-to-User Signaling (MA-UUI)
115	Space
116	Resource flag
117	Space
118-121	Packet count
122	Space
123	temporary-signaling connection (TSC) flag
124	Space
125-133	Reserved
134	Space
135	Carriage return
136	Line feed
137-139	Null

CDR data format - enhanced expanded for Communication Manager 4.0 or later

Table 34: CDR data format - enhanced expanded for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	Access code dialed
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number

Table continues…

Position	Description
49	Space
50-64	Account code
65	Space
66-72	Authorization code
73	Space
74-75	Time in queue
76	Space
77	FRL
78	Space
79-81	Incoming circuit ID
82	Space
83-85	Outgoing circuit ID
86	Space
87	Feature flag
88	Space
89-92	Attendant console
93	Space
94-97	Incoming TAC
98	Space
99-100	Node number
101	Space
102-106	ISDN NSV
107	Space
108-111	IXC
112	Space
113	BCC
114	Space
115	MA-UUI
116	Space
117	Resource flag
118	Space
119-122	Packet count
123	Space
124	TSC flag
125	Space

Table continues…

Position	Description
126-127	Bandwidth
128	Space
129-134	ISDN CC (digits 1-6)
135-139	ISDN CC (digits 7-11) / periodic pulse metering (PPM) count (1-5)
140-150	Reserved for future use
151	Carriage return
152	Line feed
153-155	Null

CDR data format - unformatted for Communication Manager 4.0 or later

Table 35: CDR data format - unformatted for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-13	Access code dialed
14-17	Access code used
18-32	Dialed number
33-42	Calling number
43-57	Account code
58-64	Authorization code
65-66	Space
67	FRL
68-70	Incoming circuit ID (hundreds, tens, units)
71-73	Outgoing circuit ID (hundreds, tens, units)
74	Feature flag
75-78	Attendant console
79-82	Incoming TAC
83-84	Node number
85-89	INS
90-92	IXC

Table continues…

Position	Description
93	BCC
94	MA-UUI
95	Resource flag
96-99	Packet count
100	TSC flag
101-104	Reserved
105	Carriage return
106	Line feed
107-109	Null

CDR data format - enhanced unformatted for Communication Manager 4.0 or later

Table 36: CDR data format - enhanced unformatted for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-13	Access code dialed
14-17	Access code used
18-32	Dialed number
33-42	Calling number
43-57	Account code
58-64	Authorization code
65-66	Space
67	FRL
68-70	Incoming circuit ID
71-73	Outgoing circuit ID
74	Feature flag
75-78	Attendant console number
79-82	Incoming TAC
83-84	Node number
85-89	ISDN NSV

Table continues…

Position	Description
90-93	IXC code
94	BCC
95	MA-UUI
96	Resource flag
97-100	Packet count
101	TSC flag
102-103	Bandwidth
104-109	ISDN CC (digits 1-6)
110-114	ISDN CC (digits 7-11)/PPM count (1-5)
115-118	Reserved for future use
119	Carriage return
120	Line feed
121-123	Null

CDR data format - int process for Communication Manager 4.0 or later

Table 37: CDR data format - int process for Communication Manager 4.0 or later

Position	Description
1-2	Format code
3-4	Time of day-hours
5-6	Time of day-minutes
7	Duration-hours
8-9	Duration-minutes
10	Duration-tenths of minutes
11	Space
12	Condition code
13	Space
14-16	Access code dialed
17-19	Access code used
20	Space
21-38	Dialed number (digits 1-18)
39-43	Calling number (digits 1-5)
44	Space
45-59	Account code (digits 1-15)
60	Space

Table continues…

Position	Description
61	IXC
62	FRL
63-65	Space
66-67	Incoming circuit ID (digits 1-2)
68-70	Space
71-72	Outgoing circuit ID (digits 1-2)
73	Space
74-78	PPM count (digits 1-5)
79	Carriage return
80	Line feed
81-83	Null

CDR data format - int-direct for Communication Manager 4.0 or later

Table 38: CDR data format - int-direct for Communication Manager 4.0 or later

Position	Description
1-2	Day of month
3-4	Month
5-6	Year
7	Space
8-9	Time of day-hours
10-11	Time of day-minutes
12	Space
13	Duration-hours
14-15	Duration-minutes
16	Duration-tenths of minutes
17	Space
18	Condition code
19	Space
20-22	Access code dialed
23-25	Access code used
26	Space
27-44	Dialed number used
45	Space
46-50	Calling number

Table continues…

Position	Description
51	Space
52-66	Account code
67	Space
68-72	PPM count
73	Space
74-75	Incoming circuit ID
76	Space
77-78	Outgoing circuit ID
79	Carriage return
80	Line feed

CDR data format - int-ISDN for Communication Manager 4.0 or later

Table 39: CDR data format - int-ISDN for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	Access code dialed
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number
49	Space
50-64	Account code
65	Space
66-72	Authorization code

Table continues…

Position	Description
73	Space
74	Line feed
75	Space
76	FRL
77	Space
78	Incoming circuit ID (hundreds)
79	Incoming circuit ID (tens)
80	Incoming circuit ID (units)
81	Space
82-84	Outgoing circuit ID
85	Space
86	Feature flag
87	Space
88-91	Attendant console (1st digit)
92	Space
93-96	Incoming trunk access code
97	Space
98-99	Node number
100	Space
101-105	INS
106	Space
107-110	IXC
111	Space
112	BCC
113	Space
114	MA-UUI
115	Space
116	Resource flag
117	Space
118-123	Reserved
124-128	PPM or reserved
129-135	Space
136	Carriage return
137	Line feed
138-140	Null

Standard CDR call record formats for “legacy” CDR

See the following tables for a description of the standard call record formats for legacy CDR:

Note:

“Legacy” CDR refers to CDR formats for releases before Communication Manager Release 4.0.

CDR data format - TELESEER for Communication Manager 3.x

Table 40: CDR data format - TELESEER for Communication Manager 3.x

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes
11	Duration-tenths of minutes
12	Condition code
13-15	Access code dialed
16-18	Access code used
19-33	Dialed number
34-38	Calling number
39-53	Account code
54	facilities restriction level (FRL)
55	inter-exchange carrier (IXC)
56-58	Incoming circuit ID
59-61	Outgoing circuit ID
62	Feature flag
63-69	Authorization code
70-76	Space
77	Carriage return
78	Line feed
79-81	Null

CDR data format - ISDN TELESEER for Communication Manager 3.x

Table 41: CDR data format - ISDN TELESEER for Communication Manager 3.x

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes
11	Duration-tenths of minutes
12	Condition code
13-15	IXC
16-18	Access code used
19-33	Dialed number
34-38	Calling number
39-53	Account code
54	INS (units)
55	FRL
56-58	Incoming circuit ID
59-61	Outgoing circuit ID
62	Feature flag
63-69	Authorization code
70-71	INS (hundreds, tens)
72-76	Space
77	Line feed
78-80	Null

CDR data format - enhanced TELESEER for Communication Manager 3.x

Table 42: CDR data format - enhanced TELESEER for Communication Manager 3.x

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes

Table continues…

Position	Description
11	Duration-tenths of minutes
12	Condition code
13-16	IXC code
17-19	Access code used
20-34	Dialed number
35-39	Calling number
40-54	Account code
55	ISDN NSV (units)
56	FRL
57-59	Incoming circuit ID
60-62	Outgoing circuit ID
63	Feature flag
64-70	Authorization code
71-72	ISDN NSV (hundreds, tens)
73-76	Space
77	Carriage return
78	Line feed
79-81	Null

CDR data format - 59 character for Communication Manager 3.x

Table 43: CDR data format - 59 character for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-12	Access code dialed
13-15	Access code used
16-30	Dialed number
31-35	Calling number
36-50	Account code
51	FRL

Table continues…

Position	Description
52	IXC
53-55	Incoming circuit ID
56-58	Outgoing circuit ID
59	Carriage return
60	Line feed
61-63	Null

CDR data format - printer for Communication Manager 3.x

Table 44: CDR data format - printer for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	Access code dialed
16	Space
17-19	Access code used
20	Space
21-35	Dialed number
36	Space
37-41	Calling number
42	Space
43-57	Account code
58	Space
59-65	Authorization code
66-69	Space
70	FRL
71	Space
72	IXC

Table continues…

Position	Description
73	Space
74-76	Incoming circuit ID
77	Space
78-80	Outgoing circuit ID
81	Space
82	Feature flag
83	Carriage return
84	Line feed

CDR data format - ISDN printer for Communication Manager 3.x

Table 45: CDR data format - ISDN printer for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	IXC
16	Space
17-19	Access code used
20	Space
21-35	Dialed number
36	Space
37-41	Calling number
42	Space
43-57	Account code
58	Space
59-65	Authorization code
66	Space
67-68	INS (hundreds, tens)

Table continues…

Position	Description
69	Space
70	INS (units)
71	Space
72	FRL
73	Space
74-76	Incoming circuit ID
77	Space
78-80	Outgoing circuit ID
81	Space
82	Feature flag
83	Carriage return
84	Line feed

CDR data format - enhanced printer for Communication Manager 3.x

Table 46: CDR data format - enhanced printer for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	IXC code
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-43	Calling number
44	Space
45-59	Account code

Table continues…

Position	Description
60	Space
61-67	Authorization code
68	Space
69-71	ISDN NSV
72	Space
73	FRL
74	Space
75-77	Incoming circuit ID
78	Space
79-81	Outgoing circuit ID
82	Space
83	Feature flag
84	Carriage return
85	Line feed

CDR data format - LSU-expand for Communication Manager 3.x

Table 47: CDR data format - LSU-expand for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	Access code dialed
16-18	Access code used
19	Space
20-34	Dialed number
35	Space
36-39	Calling number
40	Space

Table continues…

Position	Description
41-45	Account code
46	Space
47-53	Authorization code
54-57	Space
58	FRL
59	Space
60	Calling number (1st digit)
61	Space
62-63	Incoming circuit ID (tens, units)
64	Space
65	Feature flag
66	Space
67-68	Outgoing circuit ID (tens, units)
69	Space
70	Outgoing circuit ID (hundreds)
71	Space
72	Incoming circuit ID (hundreds)
73	IXC
74	Carriage return
75	Line feed
76-78	Null

CDR data format - LSU for Communication Manager 3.x

Table 48: CDR data format - LSU for Communication Manager 3.x

Position	Description
1	Duration-hours
2-3	Duration-minutes
4	Duration-tenths of minutes
5	Condition code
6-8	Access code dialed
9-11	Access code used
12-26	Dialed number
27-30	Calling number (digits 2-5 for a 5-digit dial plan)
31-35	Account code (first 5 digits)

Table continues…

Position	Description
36-42	Authorization code or digits 6-12 of the account code
43-44	Space or digits 13-14 of account code
45	FRL or digit 15 of the account code
46	Calling number (1st digit)
47-48	Incoming circuit ID (tens, units)
49	Feature flag
50-52	Outgoing circuit ID (tens, units, hundreds)
53	Incoming circuit ID (hundreds)
54	IXC
55	Carriage return
56	Line feed
57-59	Null

CDR data format - ISDN LSU for Communication Manager 3.x

Table 49: CDR data format - ISDN LSU for Communication Manager 3.x

Position	Description
1	Duration-hours
2-3	Duration-minutes
4	Duration-tenths of minutes
5	Condition code
6-8	IXC
9-11	Access code used
12-26	Dialed number
27-30	Calling number (digits 2-5 for a 5-digit dial plan)
31-35	Account code (digits 1-5)
36-42	Authorization code or digits 6-12 of the account code
43-44	INS or digits 13-14 of account code
45	INS (3rd digit), FRL, or digit 15 of the account code
46	Calling number (1st digit of a 5-digit calling number)
47-48	Incoming circuit ID (tens, units)
49	Feature flag
50-52	Outgoing circuit ID (tens, units, hundreds)
53	Incoming circuit ID (hundreds)
54	FRL

Table continues…

Position	Description
55	Carriage return
56	Line feed
57-59	Null

CDR data format - enhanced LSU for Communication Manager 3.x

Table 50: CDR data format - enhanced LSU for Communication Manager 3.x

Position	Description
1	Duration-hours
2-3	Duration-minutes
4	Duration-tenths of minutes
5	Condition code
6-9	IXC code
10-12	Access code used
13-27	Dialed number
28-31	Calling number
32-35	Account code (digits 1-4)
36-42	Authorization code or digits 6-12 of the account code
43-45	ISDN NSV
46	1st digit of a 5-digit calling number
47-48	Incoming circuit ID (tens, units)
49	Feature flag
50-52	Outgoing circuit ID (tens, units, hundreds)
53	Incoming circuit ID (hundreds)
54	FRL
55	Carriage return
56	Line feed
57-59	Null

CDR data format - expanded for Communication Manager 3.x

Table 51: CDR data format - expanded for Communication Manager 3.x

Position	Description
1-2, 3-4	Time of day-hours, -minutes
5	Space

Table continues…

Position	Description
6, 7-8, 9	Duration-hours, minutes, tenths of minute
10	Space
11	Condition code
12	Space
13-16	Access code dialed
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number
49	Space
50-64	Account code
65	Space
66-72	Authorization code
73-76	Space
77	FRL
78	Space
79-81	Incoming circuit ID
82	Space
83-85	Outgoing circuit ID
86	Space
87	Feature flag
88	Space
89-90	Attendant console
91	Space
92-95	Incoming trunk access code
96	Space
97-98	Node number
99	Space
100-102	INS
103	Space
104-106	IXC
107	Space
108	Bearer capability class (BCC)

Table continues…

Position	Description
109	Space
110	Message-Associated User-to-User Signaling (MA-UUI)
111	Space
112	Resource flag
113	Space
114-117	Packet count
118	Space
119	temporary-signaling connection (TSC) flag
120	Space
121-129	Reserved
130	Space
131	Carriage return
132	Line feed
133-135	Null

CDR data format - enhanced expanded for Communication Manager 3.x

Table 52: CDR data format - enhanced expanded for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	Access code dialed
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number

Table continues…

Position	Description
49	Space
50-64	Account code
65	Space
66-72	Authorization code
73	Space
74-75	Time in queue
76	Space
77	FRL
78	Space
79-81	Incoming circuit ID
82	Space
83-85	Outgoing circuit ID
86	Space
87	Feature flag
88	Space
89-90	Attendant console
91	Space
92-95	Incoming TAC
96	Space
97-98	Node number
99	Space
100-102	ISDN NSV
103	Space
104-107	IXC code
108	Space
109	BCC
110	Space
111	MA-UUI
112	Space
113	Resource flag
114	Space
115-118	Packet count
119	Space
120	TSC flag
121	Space

Table continues…

Position	Description
122-123	Bandwidth
124	Space
125-130	ISDN CC (digits 1-6)
131-135	ISDN CC (digits 7-11) / periodic pulse metering (PPM) count (1-5)
136-146	Reserved for future use
147	Carriage return
148	Line feed
149-151	Null

CDR data format - unformatted for Communication Manager 3.x

Table 53: CDR data format - unformatted for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-13	Access code dialed
14-17	Access code used
18-32	Dialed number
33-42	Calling number
43-57	Account code
58-64	Authorization code
65-66	Space
67	FRL
68-70	Incoming circuit ID (hundreds, tens, units)
71-73	Outgoing circuit ID (hundreds, tens, units)
74	Feature flag
75-76	Attendant console
77-80	Incoming TAC
81-82	Node number
83-85	INS
86-88	IXC

Table continues…

Position	Description
89	BCC
90	MA-UUI
91	Resource flag
92-95	Packet count
96	TSC flag
97-100	Reserved
101	Carriage return
102	Line feed
103-105	Null

CDR data format - enhanced unformatted for Communication Manager 3.x

Table 54: CDR data format - enhanced unformatted for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-13	Access code dialed
14-17	Access code used
18-32	Dialed number
33-42	Calling number
43-57	Account code
58-64	Authorization code
65-66	Time in queue
67	FRL
68-70	Incoming circuit ID
71-73	Outgoing circuit ID
74	Feature flag
75-76	Attendant console number
77-80	Incoming TAC
81-82	Node number
83-87	ISDN NSV

Table continues…

Position	Description
88-89	IXC code
90	BCC
91	MA-UUI
92	Resource flag
93-96	Packet count
97	TSC flag
98-99	Bandwidth
100-105	ISDN CC (digits 1-6)
106-110	ISDN CC (digits 7-11)/PPM count (1-5)
111-114	Reserved for future use
115	Carriage return
116	Line feed
117-119	Null

CDR data format - int process for Communication Manager 3.x

Table 55: CDR data format - int process for Communication Manager 3.x

Position	Description
1-2	Format code
3-4	Time of day-hours
5-6	Time of day-minutes
7	Duration-hours
8-9	Duration-minutes
10	Duration-tenths of minutes
11	Space
12	Condition code
13	Space
14-16	Access code dialed
17-19	Access code used
20	Space
21-38	Dialed number (digits 1-18)
39-43	Calling number (digits 1-5)
44	Space
45-59	Account code (digits 1-15)
60	Space

Table continues…

Position	Description
61	IXC
62	FRL
63-65	Space
66-67	Incoming circuit ID (digits 1-2)
68-70	Space
71-72	Outgoing circuit ID (digits 1-2)
73	Space
74-78	PPM count (digits 1-5)
79	Carriage return
80	Line feed
81-83	Null

CDR data format - int-direct for Communication Manager 3.x

Table 56: CDR data format - int-direct for Communication Manager 3.x

Position	Description
1-2	Day of month
3-4	Month
5-6	Year
7	Space
8-9	Time of day-hours
10-11	Time of day-minutes
12	Space
13	Duration-hours
14-15	Duration-minutes
16	Duration-tenths of minutes
17	Space
18	Condition code
19	Space
20-22	Access code dialed
23-25	Access code used
26	Space
27-44	Dialed number used
45	Space
46-50	Calling number

Table continues…

Position	Description
51	Space
52-66	Account code
67	Space
68-72	PPM count
73	Space
74-75	Incoming circuit ID
76	Space
77-78	Outgoing circuit ID
79	Carriage return
80	Line feed

CDR data format - int-ISDN for Communication Manager 3.x

Table 57: CDR data format - int-ISDN for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	Access code dialed
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number
49	Space
50-64	Account code
65	Space
66-72	Authorization code

Table continues…

Position	Description
73	Space
74	Line feed
75	Space
76	FRL
77	Space
78	Incoming circuit ID (hundreds)
79	Incoming circuit ID (tens)
80	Incoming circuit ID (units)
81	Space
82-84	Outgoing circuit ID
85	Space
86	Feature flag
87	Space
88-89	Attendant console (1st digit)
90	Space
91-94	Incoming trunk access code
95	Space
96-97	Node number
98	Space
99-101	INS
102	Space
103-106	IXC
107	Space
108	BCC
109	Space
110	MA-UUI
111	Space
112	Resource flag
113	Space
114-119	Reserved
120-124	PPM or reserved
125-131	Space
132	Carriage return
133	Line feed
134-136	Null

Call detail record field descriptions

The following information describes the CDR data that the system collects for each call, and the length of each field. The information is right adjusted in the **CDR record** field, unless otherwise indicated. The system displays the customized field name if the field names for the customized differ from the names of standard records.

Access Code Dialed

Customized field name: **code-dial**

Length: 3 or 4 digit

This field contains the access code that the user dials to place an outgoing call. The access can be the automatic route selection (ARS) access code, an Automatic Alternate Routing (AAR) access code, or the access code of a specific trunk group. This field is also used to record the X.25 Feature Access Code of an outgoing X.25-addressed call.

Access Code Used

Custom field name: **code-used**

Length: 3 or 4 digits

This field is used only for outgoing calls when the system uses a trunk group that differs from the access code that the user dials. This field is not used when a user dials a TAC. For example, your system might use an FAC for ARS. This field contains the access code of the trunk group that the system uses to route the call. When the access code that the user dials, and the access code that the systems uses are the same, this field is blank.

If you use ISDN or enhanced formats with TELESEER, LSU, or printer record types, this field contains the access code of the trunk group, even if the user dials the same access code.

Length: 2 digits

If an attendant participates in a call, this field contains the number of the attendant console.

Account Code

Custom field name: **acct-code**

Length: 1 to 15 digits

This field is either blank, or contain a number to associate call information with projects or account numbers. For some formats, a long account code overwrites spaces on the record that are assigned to other fields.

Attendant Console

Custom field name: **attd-console**

Length: 2 digits

If a user uses an attendant to make a call, the **attd-console** field displays the console number of the attendant. If multiple attendants are used, the console number of the last attendant is recorded. For incoming and non operator-handled calls, this field remains blank.

Authorization Code

Custom field name: **auth-code**

Length: 4 to 13 digits

This field contains the authorization code that the user used to make the call. The system truncates an authorization code to 7 digits for formats other than customized formats.

Note that the authorization code for the non-ISDN format and the ISDN local storage init (LSU) format has fewer than 6 digits. The authorization code for the Enhanced LSU format has 5 digits. The system does not record the authorization on the 59-character record.

Bandwidth

Length: 2 digits

This field contains the bandwidth of the wide band calls to support H0, H11, H12, and N x 64 kbps data rates. For Enhanced Expanded, Enhanced Unformatted, and customized record formats, this value in this field is the number of DSOs of 64-kbps channels that comprise a call.

Bearer Capability Class

Custom field name: **bcc**

Length: 1 digit

This field contains the bearer capability class (BCC) for ISDN calls. The BCC identifies various capabilities that are available for a ISDN call. Any one of the following BCCs can appear in this field.

0 - Voice grade data and voice

1 - Mode 1, 56 kbps synchronous data

2 - Mode 2, less than 19.2 kbps synchronous or asynchronous data

3 - Mode 3, 64 kbps data for Link Access Procedure data (LAPD) protocol

4 - Mode 0, 64 kbps data clear

M - Multimedia

W - Wideband

Note:

The **Bearer Capability Class** field in the CDR records shows the capabilities that are available for a given call. It is not a report of the capabilities that were used for the call. For intraswitch CDR records, the BCC field system provides information for wideband calls only.

Calling Number

Custom field name: **calling-num**

Number of digits, standard: 1 to 10

Number of digits, custom: 1 to 15

For outgoing or intraswitch calls, this field contains the extension of the originating telephone user. For incoming and tandem calls, this field contains the TAC in standard formats. The fifth digit is the first digit of a 5-digit dialing plan.

For formats in which the Calling Number field has 7 digits, the field contains the TAC of the incoming call.

For Unformatted records or Expanded records, this field contains the number of the calling party. If the number of the calling party is unavailable, this field is blank for both the Unformatted and the Expanded record formats.

For an outgoing, or an originating, NCA-TSC CDR record, this field contains the local extension of the noncall-associated/temporary-signaling connection (NCA-TSC) endpoint. This field is blank for terminating, tandem, or unsuccessful NCA-TSC CDR records.

Call Type

Custom field name: **calltype**

Length: 1 digit

This field is only used in the customized format and is used to indicate whether the called party number was handled by calltype digit analysis or not. If the call was handled by calltype digit analysis, the field is set to a 1, otherwise it is set to a 0. This field was formerly called logdial.

Calling Number/Incoming TAC

Custom field name: **clg-num/in-tac**

You can use this field on a customized record to display the calling number, if the calling number is available.

If the calling party number is unavailable, this field contains the incoming TAC.

For outgoing calls, this field contains the calling extension.

Calling Party Category

Custom field name: **clg-pty-cat**

Length: 2 digits

This field is used only on the customized format. This parameter is associated with R2MFC trunks.

Carriage Return

Custom field name: **return**

The ASCII carriage return character, followed by a line feed, indicates the end of a call record.

Condition Code

Length: 1 character

The condition code indicates the type of call that this record describes. For example, condition code C identifies a conference call, and condition code 7 identifies an ARS call.

The table on page 441 shows the condition codes for most record formats. The condition codes for the 59-character format differ from the condition codes of the other record types. The codes that apply to 59-character records appear in parentheses in the table.

Table 58: Condition codes

Condition codes	Description
0	Identifies an intraswitch call, which is a call that originates and terminates on the switch

Table continues…

Condition codes	Description
1 (A)	Identifies an attendant-handled call or an attendant-assisted call, except conference calls
4 (D)	Identifies an extremely long call or a call with an extremely high message count TSC. An extremely long call is a call that lasts for 10 or more hours. An extremely high message count TSC is 9999 or more messages. When a call exceeds10 hours, the system creates a call record with this condition code and a duration of 9 hours, 59 minutes, and 1-9 tenths of a minute. The system creates a similar call record with this condition code after each succeeding 10-hour period. When the call terminates, the system creates a final call record with a different condition code that identifies the type of call.
6 (E)	Identifies calls where no CDR records are generated because the CDR (SMDR) processes do not have enough resources available to generate a record. For example, a CDR resource shortage could be the CDR buffer space available. The CDR record that includes this condition code also includes the time and the duration of the CDR resource outage.
7 (G)	Identifies calls that use the AAR or ARS feature.
8 (H)	Identifies calls that are served on a delayed basis by the Ringback Queuing feature.
9 (I)	Identifies: • An incoming call • A tandem call • An incoming NCA-TSC call • A tandem NCA-TSC call
A	Identifies an outgoing call.
B	Identifies an adjunct-placed outgoing call.
C (L)	Identifies a conference call. For trunk CDR, the system creates a separate call record, with this condition code, for each incoming or outgoing trunk that is used during the conference call. If you disable ITCS and OTCS, the system records the extension of the originator of the conference call. The system does not record any other extension. If you disable ITCS, and you administer the originator of the conference call to use Intraswitch CDR, the system generates a call with this condition code whenever the originator of the conference dials a nontrunk conference participant. If ITCS is active, and you do not administer the originator of the conference call to use Intraswitch CDR, the system generates a call with this condition code whenever the originator of the conference dials an intraswitch conference participant.

Table continues…

Condition codes	Description
E (N)	Identifies a call that the system does not complete because the following facilities to complete the call are unavailable: • Outgoing calls - The trunks are busy, and no queue exists. - The trunks are busy, and the queue is full. • Incoming calls - The extension is busy. - The extension is unassigned. This condition code also identifies an ISDN Call By Call Service Selection call that is unsuccessful because of an administered trunk usage allocation plan. Incoming trunk calls to a busy telephone do not generate a CDR record.
F	Identifies a call that the system does not complete because of one of the following conditions: • The originator of the calls has insufficient calling privileges. • An NSF mismatch occurs for an ISDN call. • An authorization mismatch occurs for a data call.
G	Identifies a call that the system terminates to a ringing station.
H	Notes that the system abandoned a ringing call.
I	Identifies a call that the system terminates to a busy station.
J	Identifies an incoming trunk call that is a new connection that uses Additional Network Feature-Path Replacement (ANF-PR) or DCS with Rerouting. For more information on QSIG and ANF-PR, see *Administering Avaya Aura® Communication Manager*.
K	Identifies an outgoing trunk call that is a new connection that uses ANF-PR or DCS with Rerouting. For more information on QSIG and ANF-PR, see *Administering Avaya Aura® Communication Manager*.
M	Identifies an outgoing trunk calls that the system disconnects because the call exceeds the allotted time.
T	Identifies CDR records for calls that meet the following conditions: • The **Condition Code 'T' for Redirected Calls?** field on the CDR System Parameters screen is set to y. • The incoming trunk group is direct inward dialing (DID). • The system automatically redirects an incoming call off of the server.
O	Identifies CDR records for all calls in which URI was used as dialed digits.
P	Identifies CDR records for all calls in which SA8957 PIN code for Private Calls was used.

If the **Trunk-group CDR Reports** field is set to ring, CDR records the ring time to answer or abandon for incoming calls that the trunk group originates. CDR also indicates if the incoming

destination is busy. This record is separate from the normal call duration record that is printed for an answered call. This information is indicated by the condition code.

When a trunk group originates an incoming call with this option set that is terminated to an internal destination, the call is tracked from the time that ringing feedback is given to the originator. If the call is answered, a CDR record is printed with condition code G, and the duration reflects the time between the start of ringing and when the call is answered. If the call is abandoned before being answered, the system prints a record with condition code H, and the duration reflects the time between the start of ringing and the time that the call was abandoned. If the destination is busy, a CDR record is printed with condition code I and a duration of 0.

Condition code overrides

If two condition codes apply to the same call, one code overrides the other. The following matrix, the table on page 444, defines the overrides.

To use this table, locate one of the condition codes that you want to compare in the row of condition codes at the top of the table. Then locate the other condition code that you want to compare in the column of condition code at the far left of the table. Then locate the intersection of these two condition codes. The condition code at the intersection of the two condition codes, is the condition code that the system uses. For example, assume that the system can assign condition 7 and condition code A to the same call. The system uses condition code 7 for the call.

If the intersection of the two condition codes contains a dash, the two conditions never occur for the same call.

Table 59: Condition code override matrix

Condition codes																
	0	**1**	**4**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**E**	**F**	**J**	**K**	**M**	**T**
0	-	0	4	6	0	-	-	-	B	C	-	-	-	-	-	-
1	0	-	4	6	1	-	9	1	B	C	E	-	J	K	-	-
4	4	4	-	6	4	4	4	4	4	4	-	-	J	K	-	-
6	6	6	6	-	6	6	6	6	6	6	6	6	6	6	-	-
7	0	1	4	6	-	7	9	7	B	C	E	F	J	K	-	-
8	-	-	4	6	7	-	-	8	B	C	E	-	-	K	-	-
9	-	9	4	6	9	-	-	-	-	C	E	F	-	-	-	-
A	-	1	4	6	7	8	-	-	B	C	E	F	-	-	-	-
B	B	B	4	6	B	B	-	B	-	B	E	F	-	K	-	-
C	C	C	4	6	C	C	C	C	B	-	-	-	J	K	M	-
E	-	E	-	6	E	E	E	E	E	-	-	-	E	E	-	-
F	-	-	-	6	F	-	F	F	F	-	-	-	F	F	-	-
J	-	J	J	6	J	-	-	-	-	J	E	F	-	-	-	-
K	-	K	K	6	K	K	-	-	-	K	E	F	-	-	-	-
M	-	-	-	-	-	-	-	-	-	M	-	-	-	-	-	-
T	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Contact Uniform Resource Identifier

Custom field name: **contact-uri**

Length: 20 digits

The **Contact-URI** field contains the Uniform Resource Identifier (URI) associated with the calling party on a SIP call. This field is used only with the customized format. The Contact header contains the IP address of the machine or telephone that the call originated from. This header remains the same throughout the entire call.

Country From

Custom field name: **country-from**

Number of digits: 3

The **country-from** field is a country number, used with the Multinational Locations feature, for currency conversion. The field length is 3, the same as the length of the **Country code for CDR** field on the Location Parameters screen. The **country-from** field indicates the administered CDR country code of the PBX interface of the calling party.

Country To

Custom field name: **country-to**

Number of digits: 3

The **country-to** field is a country number, used with the Multinational Locations feature, for currency conversion. The field length is 3, the same as the length of the **Country code for CDR** field on the Location Parameters screen. The **country-to** field indicates the administered CDR country code of the PBX interface of the called party.

Note:

If the Multinational Locations feature is turned off in the license file, the key words country-from and country-to are invalid.

Date

You can include the date in customized CDR records only. The format of the date is based on the value of the **CDR Date Format** field on the CDR System Parameters screen.

Dialed Number

Custom field name: **dialed-num**

Length: 23 digits

For an outgoing call, this field contains the number that the system user dials. For an incoming call, this field contains the extension of the system user that is called. If a Dialed Number Identification System (DNIS) exists, the field contains the implied extension for an incoming call. If the originator of the call dials more than eighteen digits, the system truncates the number or the extension to 18 digits. The system truncates the least significant digits, starting at the right. For example, if the originator of the call dials the number 11111111111111111852, the system truncates the digits 852.

- CDR Privacy

If CDR Privacy is active for the calling number, and this CDR record is for an outgoing call, the system modifies and records the number that the user dials according to the following procedure:

- The system truncates the numbers that the user dials to 18 digits
- The system replaces some of the digits with blanks to ensure the privacy of the call.

- NCA-TSC or tandem NCA-TSC outgoing calls

  For outgoing NCA-TSC or tandem NCA-TSC calls, this field contains the digits that the user dials, and that the system uses to establish a route to the server.

  The field contains the local extension that is used as the NCA-TSC endpoint when the extension is for a terminating NCA-TSC. For an unsuccessful NCA-TSC outgoing call, this field is blank.

  The field can contain a pound sign (#) or the letter E for either ARS calls or TAC calls when:

- A user dials a pound sign (#) at the end of a string of digits
- An outgoing call exceeds the interdigit-timeout interval that is in the ARS Analysis table
- A user makes a TAC call, which then routes through Look Ahead Interflow (LAI). For example, a successful LAI to <TAC> 1001, where 1001 is the remote VDN extension, yields 1001E or 1001# in the Dialed Number field. The vector processing software uses the pound sign (#) or E to indicate the end of the string of digits that the user dials.

  You administer the CDR System Parameter screen so the pound sign (#) or the letter E need not be the last digit of the CDR record.

Duration

Custom field name: **duration** or **sec-dur**

Length: 4 digits

This field contains the duration of the call, which the system records in hours (0 to 9), minutes (00 to 59), and tenths of minutes (0 to 9). The system rounds the duration of the call down in 6-second increments. For example, the system records the duration of a 5-second call as a duration of zero. If this field contains the value 9999, the call was in progress when a time change was made in the switch.

You can use the customized record format to report the duration of the call in hours, minutes, and seconds.

end-date(4d)

Length: 8 digits

This field is associated with Special Application SA8201. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to Special Application features.

Feature Flag

Custom field name: **feat-flag**

Length: 1 digit

The feature flag indicates whether a call received network answer supervision, and whether the call was interworked in the network. The duration of the call starts when the system receives the network answer.

You can administer the **Feature flag** field on the CDR System Parameters screen to reflect whether the network reported an outgoing ISDN call as interworked.

- The number 0 in this field indicates either a voice call without network answer supervision or a call for which NCA-TSC is not established.
- The number 1 in this field indicates a data call without network answer supervision.
- The number 2 in this field indicates a voice call with network answer supervision, but interworked.
- The number 3 in this field indicates a data call with network answer supervision, but interworked.
- The number 4 in this field indicates a voice call with network answer supervision.
- The number 5 in this field indicates a data call with network answer supervision.

  The time of the answer and the duration of the call are accurate if the feature flag indicates that the call received network answer supervision.

  The time of the answer and the duration of the call can be inaccurate, if the call does not receive network answer supervision, or the call receives answer supervision but is interworked with non-ISDN trunks.

  Calls are considered data calls if the calls use a conversion resource, such as a modem, and the calls either originate or terminate on a data module.

Format Code

Length: 2 digits

This field contains two values:

- 00 indicates no PPM.
- 03 indicates a PPM count in the digits record.

FRL

Length: 1 digit

Facilities restriction levels (FRLs) are numbered 0 through 7, are associated with the AAR and the ARS features, and define calling privileges. If the call is an:

- Outgoing call, and an authorization code is not used to make the call, this field contains the FRL of the originating user FRL.
- Outgoing call, and an authorization code is used to make the call, this field contains the FRL that is associated with the authorization code that the user dials.
- Incoming or a tandem call, this field contains the FRL that is assigned to the incoming trunk group.
- Incoming tandem tie trunk call, this field contains either the FRL that is assigned to the tandem tie trunk or the TCM sent with the tandem tie trunk call. If an FRL was used to complete the call, the field contains the FRL. If a TCM was used to complete the call, the

field contains the TCM. With ISDN calls, this field always contains the TCM, if the TCM was received.

You can administer CDR so that this field contains disconnect information instead of the FRL. If you administer CDR so this field contains disconnect information for trunk CDR, the system records the information shown in the table on page 448.

Table 60: Disconnect information for trunk CDR

Data	Meaning
0	The system cannot determine which participant on the call dropped the call first.
1	The switch participant dropped the call first.
2	CO participant dropped the call first.
3	Maintenance seized the trunk

For intraswitch CDR, the field contains the information that is shown in the table on page 448 instead of the FRL.

Table 61: Intra-switch CDR call disconnect information

Data	Meaning
0	The system cannot determine which participant on the call dropped the call first.
1	The calling participant dropped the call first.
2	The dialed participant dropped the call first.

From-URI

Length: 20 digits

The **From-URI** field contains the URI associated with the calling party on a SIP call. This field is used only with the customized format. The From header contains the caller ID information. This header can contain ID information that the calling party wants the header to contain. The ID information might or might not be accurate and therefore is not considered to be a reliable source of information.

Note:

To have a more consistent and repeatable information in the CDR records, use the **Contact-URI** field instead of the **From-URI** field.

Incoming Circuit Identification

Custom field name: **in-crt-id**

Length: 3 digits

This field contains the member number of a trunk within a trunk group that is used for an incoming call. For outgoing calls, this field is blank. Tandem calls contain both incoming and outgoing circuit ID numbers.

The format of this field varies from record to record. For printer, TELESEER, and 59-character formats, the numbers are inverted on the record. For example, the system displays the circuit ID 123 as 231 (tens, units, hundreds). If you want to change the order to hundreds, tens, units format, for example, 123, use the **Modified Circuit ID Display** field on the CDR System Parameters screen.

From Communication Manager Release 8.0 onwards, maximum trunk capacity is increased to 9999. However, for the fixed CDR formats such as TELESEER, unformatted, and 59-character, there is a limitation of the field length to three digits only. So this field will always report lower three digits only for fixed CDR format. If you want all the four digits, then you must use custom format. The maximum trunk capacity prior to Communication Manager Release 8.0 is 255.

Incoming TAC

Custom field name: **in-trk-code**

Length: 4 digits

This field contains the access code of the incoming trunk group.

INS

Length: 3 digits

This field specifies the ISDN Network Service (INS) that is requested for a call. This field applies only to ISDN calls. Each network specific facility has a corresponding INS value, shown in the table on page 449.

The system displays this field also as ISDN NSV (network service value).

Table 62: Network-specific facility to INS mapping

Network specific facility	INS value
OUTWATS Band 0	33
OUTWATS Band 1-255	34-288
Network Operator	324
Pre subscribed Common Carrier Operator	325
Software Defined Network (SDN)	352
MEGACOM 800	353
MEGACOM	354
INWATS	355
Maximum Banded WATS	356
ACCUNET Digital Service	357
AT&T Long Distance Service	358
International 800	359
Multiquest	367

Internal Codec

Custom field name: **internal-codec**

Length: 2 digits

This field is associated with Special Application SA8702. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to Special Application features.

ISDN CC

The call charge that the ISDN advice of charge function supplies.

ISDN Call Charge/Periodic Pulse Metering

Custom field name: **isdn-cc/ppm**

Length: 11 digits

This field is used only on the customized format.

ISDN NSV

See INS.

IXC Code

The length for non-ISDN formats: 1 digit hexadecimal

Interexchange Carrier (IXC) codes,1-F hexadecimal, indicate the carrier used on the call. This information is sent to the CDR output device in ASCII code as a hexadecimal representation, for example, ASCII F equals 15 that is.

Users must dial an IXC access number to access a specific common carrier for a call. In the US, this number is in the form 10XXX, 950 - 1XXX, or any 8 to 11 digit number. The IXC access numbers that are applicable at a given location are associated with an IXC code on the Inter-Exchange Carrier Codes screen.

When ARS is used, and a route pattern inserts one of the administered IXC codes, the report contains the associated IXC code. If no IXC access number is used, or the carrier is selected at the central office (CO), the report contains a zero.

Length for ISDN formats: 3 or 4 digits

With an ISDN record format, this 3-digit or 4-digit field identifies the actual IXC used on an ISDN call. This information is determined from the route pattern administration. For AAR and ARS calls, the 3-digit IXC value is administered in the route pattern for all ISDN calls. If a user dials an IXC code with a 10XXX format as administered on the Inter-Exchange Carrier Codes screen, the CDR record contains only the last 3 digits (4 digits or Enhanced). If a user dials a 7-digit IXC code, this field contains a zero.

Line Feed

Length: 1 character

The ASCII line feed character comes after a carriage return to terminate CDR records.

Location From

Custom field name: **location-from**

Number of digits: 3

The **location-from** field is a location number, used with the Multinational Locations feature, for record sorting. The field length is 3, the same as the length of the **location** field on the cabinet, media gateway, remote office, and ip-network region screens. The **location-from** field indicates the location code of the PBX interface of the calling party.

Location To

Custom field name: **location-to**

Number of digits: 3

The **location-to** field is a location number, used with the Multinational Locations feature, for record sorting. The field length is 3, the same as the length of the **location** field on the Media Gateway and IP Network Region screens. The **location-to** field indicates the location code of the PBX interface of the called party.

Note:

If the Multinational Locations feature is turned off in the license file, the key words location-from and location-to are invalid.

MA-UUI

Length: 1 digit

Message Associated User-to-User Signaling shows the number of ISDN messages that contain user data that are sent on an outgoing call. This field contains a number from 0 to 9.

Node Number

Custom field name: **node-num**

Length: 2 digits

This field identifies the DCS node number of a switch within a DCS arrangement. This number is the local ID, which is the same as the node number on the Dial Plan screen.

Null

Length: 1 character

The Null character, usually in triplets, is used to terminate and divide CDR Records, when a receiving adjunct needs a record divider or terminator.

Outgoing Circuit Identification

Custom field name: **out-crt-id**

Length: 3 digits

For outgoing calls, this field contains the member number of the trunk within a trunk group that is used on the call. This field is blank for incoming calls. Tandem calls include both incoming and outgoing circuit ID numbers. For outgoing and tandem NCA-TSCs, this field contains the signaling group that is used to carry the NCA-TSC.

The format of this field varies from record to record. For printer, TELESEER and 59-character formats, and the ISDN and Enhanced forms of those records, the numbers are inverted on the record. For example, the system displays the circuit ID 123 as 231 (tens, units, hundreds). If you want to change the order to hundreds, tens, units format, for example, 123, use the **Modified Circuit ID Display** field on the CDR System Parameters screen.

From Communication Manager Release 8.0 onwards, maximum trunk capacity is increased to 9999. However, for the fixed CDR formats such as TELESEER, unformatted, and 59-character, there is a limitation of the field length to three digits only. So this field will always report lower three digits only for fixed CDR format. If you want all the four digits, then you must use custom format. The maximum trunk capacity prior to Communication Manager Release 8.0 is 255.

Packet Count

Custom field name: **tsc_ct**

Length: 4 digits

For ISDN TSCs, this field contains the number of ISDN-PRI USER INFO messages that are sent, received, or, for tandem TSCs, passed through the switch.

PPM

Periodic Pulse Metering (PPM) contains the pulse counts that are transmitted over the trunk line from the serving CO. The pulse counts are used to determine call charges.

Request Uniform Resource Identifier

Custom field name: **request-uri**

Length: 20 digits

The **Request-URI** field contains the URI associated with the called party on a SIP call. This field is used only with the customized format. Request-URI contains the destination of the request.

Resource Flag

Custom field name: **res-flag**

Length: 1 digit

This field indicates whether a conversion resource was used, or if the call involved a Multimedia Application Server Interface (MASI) terminal or MASI trunk, or if a video or wideband codec was used.

- 0 indicates no conversion device used, no video or wideband codec and no MASI devices
- 1 indicates wideband audio codec used
- 2 indicates conversion device used
- 4 indicates video codec used
- 5 indicates video codec and wideband audio codec used
- 8 indicates a MASI call
- indicates a MASI call with a conversion device used

Note:

Video or wideband takes precedence over MASI/conversion. If video or wideband is used, the field does not indicate if MASI or a conversion device was used.

Sec-dur

For customized records only, you can uses this field to set the duration field to record seconds instead of tenths of minutes.

seq-num

Length: 10 digits

This field is associated with Special Application SA8702. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to Special Application features.

Space

Length: 0 to 40 characters

The ASCII space character separates other CDR fields or fills unused record locations.

start-date

Length: 6 digits

This field is associated with Special Application SA8201. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to Special Application features.

start-date(4d)

Length: 8 digits

This field is associated with Special Application SA8201. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to Special Application features.

start-time

Length: 6 digits

This field is associated with Special Application SA8201. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to Special Application features.

Time

This fields contains the time that the call ended, or if Call Splitting is active, the time that a user dropped from a multiparty call.

Timezone From

Custom field name: **timezone-from**

Number of digits: 5

The **timezone-from** field is a time zone offset number, used with the Multinational Locations feature, for call time. The field length is 5, the same as the length of the **timezone offset** field on the Media Gateway and IP Network Region screens. The **timezone-from** field indicates the timezone offset of the PBX interface of the calling party.

Timezone To

Custom field name: **timezone-to**

Number of digits: 5

The **timezone-to** field is a time zone offset number, used with the Multinational Locations feature, for call time. The field length is 5, the same as the length of the **location** field on the Locations

screen. The **timezone-to** field indicates the timezone offset of the PBX interface of the called party.

Note:

If the Multinational Locations feature is turned off in the license file, the key words timezone-from and timezone-to are invalid.

To-URI

Length: 20 digits

The **To-URI** field contains the URI associated with the called party on a SIP call. This field is used only with the customized format. The To header contains the originating endpoint view of the dialed number and remains the same during the duration of the call.

TSC-Count

Custom field name: **tsc_ct**

Length: 4 digits

This field is the customized name for Packet Count. See Packet Count for more information.

TSC Flag

Custom field name: **tsc_flag**

Length: 1 digit

This field describes call records that pertain to temporary signaling connections. When the value of this field is not equal to zero, this field indicates the status of the TSC. The table on page 454 shows the TSC flag encoding.

Table 63: Encoding for the TSC flag

Code	Description
0	Circuit-switched call without TSC requests
1-3	Reserved
4	Call Associated TSC requested and accepted in response to SETUP, no congestion control (applicable to originating node). Call Associated TSC received and accepted by SETUP, no congestion control (applicable to terminating node).
5	Call Associated TSC received and accepted by SETUP, congestion control (applicable to terminating node).
6	Call Associated TSC requested, accepted after SETUP, no congestion control (applicable to originating node). Call Associated TSC received and accepted after SETUP, no congestion control (applicable to terminating node).
7	Call Associated TSC received and accepted after SETUP, congestion control (applicable to terminating node).
8	Call Associated TSC requested, rejected (rejection came from outside the local switch).

Table continues…

Code	Description
9	Call Associated TSC requested, rejected (rejection came from the local switch, that is, lack of resource).
A	Non-call-associated (NCA) TSC received, accepted, no congestion control (applicable to terminating node). NCA TSC received, accepted, no congestion control (applicable to terminating node).
B	NCA TSC requested, accepted, congestion control (applicable to originating node). NCA TSC received, accepted, congestion control (applicable to terminating node).
C	NCA TSC requested, rejected (rejection came from outside the local switch).
D	Non Call Associated TSC requested, rejected (rejection came from the local switch, that is, lack of resource).
E	Reserved for future use.
F	Reserved for future use.

trunk-codec

Length: 2 digits

This field is associated with Special Application SA8702. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to Special Application features.

ucid

Length: 20 digits

This field is associated with Special Application SA8702. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to Special Application features.

VDN

Custom field name: **vdn**

Length: 16 digits

This field is available on customized records only. The call record contains the VDN extension number. If VDN Return Destination is active, this field contains the first VDN that the caller accessed.

Call Detail Recording administration

The following tasks are part of the administration process for the Call Detail Recording feature:

- Assigning Forced Entry of Account Codes for CDR
- Assigning privacy digits for a user for CDR
- Administering the CDR system parameters
- Administering CDR for a trunk group

- Administering CDR for a data module
- Identifying the Inter Exchange Carrier for CDR groups
- Administering CDR for the paging ports
- Administering the Intra-Switch CDR
- Administering Survivable CDR
- Enabling CDR for Extension to Cellular
- Changing configuration sets for Extension to Cellular

Related links

Assigning Forced Entry of Account Codes for CDR on page 457
Assigning privacy digits for a user for CDR on page 458
Administering the CDR system parameters on page 459
Administering CDR for a trunk group on page 467
Administering CDR for a data module
Identifying the Inter Exchange Carrier for CDR records on page 470
Administering CDR for the paging ports on page 470
Administering the Intra-Switch CDR on page 470
Administering Survivable CDR on page 471
Enabling CDR for Extension to Cellular on page 784
Changing configuration sets for Extension to Cellular on page 785

Preparing to administer Call Detail Recording

About this task

- Ensure that the CDR account code feature is available on your system.
  1. Type `change feature-access-codes`. Press `Enter`.

     The system displays the Feature Access Codes (FAC) screen.
  2. In the **CDR Account Code Access Code** field, type the code that you want a user to enter before the user enters a CDR account code number. For more information, see the Feature Access Code feature.
  3. Press `Enter` to save your changes.
- Ensure that call classification is enabled on your system.
  1. Type `display system-parameters customer-options`. Press `Enter`.

     The system displays the Optional Features screen.
  2. Ensure that the **Answer Supervision by Call Classifier** field is set to y.

     If the **Answer Supervision by Call Classifier** field is set to n, your system does not support call classification. Go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, and knowledge articles related to administering Call Detail Recording, or to open a service request.

Assigning Forced Entry of Account Codes for CDR

Assigning FEAC for all calls for CDR

Before you begin

- Type `display System-Parameters Customer-Options` to view the Optional Features screen. Press `Enter`.

  Ensure that the **Forced Entry of Account Codes** field is set to y. If the **Forced Entry of Account Codes** field is set to n, your system does not support FEAC for all calls. If you want to use FEAC for all calls, go to the Avaya Support website at http://support.avaya.com to open a service request.

Procedure

1. Type `change system-parameters cdr`. Press `Enter`.

   The system displays the CDR System Parameters screen.

2. In the **Force Entry of Acct Code for Calls Marked on Toll Analysis Form?** field, perform one of the following actions:

   - If you want the system to require that a user enter an account code for all calls, type `y`.
   - If you do not want the system to require that a user enter an account code for all calls, type `n`.

   Note:

   The information in the **Force Entry of Acct Code for Calls Marked on Toll Analysis Form?** field does not override other call restrictions that the user might have.

Assigning FEAC to a COR for CDR

Procedure

1. Type `change cor` *n*, where *n* is the number of the COR to which you want to assign FEAC. Press `Enter`.

   The system displays the Class of Restriction screen.

2. In the **Forced Entry of Account Codes** field, perform one of the following actions:

   - If you want all users to enter an account code for calls that require an account code, type `y`.
   - If you do not want all users to enter an account code for calls that require an account code, type `n`.

3. Press `Enter` to save your changes.

Assigning FEAC to a user for CDR

Procedure

1. Type `change station n`, where *n* is the number of the user extension to which you want to assign FEAC. Press `Enter`.

   The system displays the Station screen.

2. In the **COR** field, type the number of the COR that requires the user to enter an account code.
3. Press `Enter` to save your changes.
4. Type `change trunk-group n`, where *n* is the number of the trunk group to which you want to assign FEAC. Press `Enter`.

   The system displays the Trunk Group screen.

5. In the **COR** field, type the number of the COR that requires a user to enter an account code for calls that use this trunk group.
6. Press `Enter` to save your changes.

Assigning privacy digits for a user for CDR

Assigning the system-wide privacy digits

Procedure

1. Type `change system-parameters cdr`. Press `Enter`.

   The system displays the CDR System Parameters screen.

2. In the **Privacy - Digits to Hide** field, type the number of user-dialed digits that the system replaces with blanks when the system generates a CDR record of the call.
3. Press `Enter` to save your changes.

Assigning CDR privacy to a user:

Procedure

1. Type `change station n`, where *n* is the number of the user extension to which you want to assign CDR privacy. Press `Enter`.
2. On the Station screen, click `Next` until you see the **CDR Privacy?** field.
3. In the **CDR Privacy?** field, perform one of the following actions:
   - If you want the system to replace some of the digits that the user dials, when the system generates a CDR record of the call, type `y`.
   - If you do not want the system to replace some of the digits that the user dials, when the system generates a CDR record of the call, type `n`.
4. Press `Enter` to save your changes.

Administering the CDR system parameters

Procedure

1. Type `change system-parameters cdr`. Press `Enter`.

   The system displays the CDR System Parameters screen.

2. In the **Inc Trk Call Splitting** field, perform one of the following actions:

   - Type `y` if you want the system to create separate records for each portion of an incoming call that is transferred or conferenced.
   - Type `n` if you do not want the system to create separate records for each portion of an incoming call that is transferred or conferenced.

   Note:

   The system only displays this field when the **Record Outgoing Calls Only** field on the System Parameters CDR screen is set to n.

3. In the **Record Outgoing Calls Only** field, perform one of the following actions:

   - Type `y` if you only want the system to record outgoing calls.
   - Type `n` if you want the system to record both incoming and outgoing calls.

4. In the **Call Record Handling Option** field, perform one of the following actions:

   - Type `reorder` if you want the system blocked calls to generate reorder tone, when the buffer is full. If you choose this option, no one can make or receive calls if the system cannot generate CDR records for the calls.
   - Type `warning` if you want the system to stop recording calls when the buffer is full. If the buffer is full, and you choose this option, the system generates a minor alarm.

     The default value for this field is warning. Note that if you change the default, the system might redirect the ACD calls and the vector calls the system records for CDR.
   - Type `attendant` if you want the system to route all the calls to the attendant as non-CDR calls.

     Note:

     If you change the system default of warning, ACD calls and vector calls that are measured by CDR might be redirected. Also, the system displays the **Call Record Handling Option** field only for DEFINITY R.

     The system uses the information in this field to control call routing when:

     - New calls come in.
     - The CDR link is not operating.
     - The buffer is full.

5. In the **Calls to Hunt Group-Record** field, perform one of the following actions:
   - Type `member-ext` if you want the system to record the extension of the telephone or data terminal where the call terminates.
   - Type `group-ext` if you want the system to record the extension that the user dials.
6. In the **CDR Account Code Length** field, type the number of digits that you want the system to record when a user enters an account code.

   For some record formats, the system overwrites the information in other fields if the account code is too long.
7. In the **CDR Date Format** field, perform one of the following actions:
   - Type `month/day` if you want to use the month and day date format for the date stamp that starts each new day of call records.
   - Type `day/month` if you want to use the day and month date format for the date stamp that starts each new day of call records.
8. In the **Condition Code 'T' for Redirected Calls** field, perform one of the following actions:
   - Type `y` if you want the system to record condition code T for both CDR records of the call that the system automatically redirects off the server that runs Communication Manager.
   - Type `n` if you want the system to record the condition codes that are usually associated with the **Record Outdoing Call Only** field for calls that the system automatically redirects off the server that runs Communication Manager.
9. In the **Digits to Record for Outgoing Calls** field, perform one of the following actions:
   - Type `dialed` to record the digits that a user dials.
   - Type `outpulsed` to record the digits that the software actually sends out over the trunk. This information includes any additions or deletions that take place during routing.
10. In the **Disconnect Information in Place of FRL** field, perform one of the following actions:
    - Type `y` if you want the system to replace the **Facility Restriction Level (FRL)** field with the call disconnect information. You can use the call disconnect information to isolate problems between the DEFINITY R and the telephone network.
    - Type `n` if you want the system to record the facilities restriction level (FRL) of the call.
11. In the **EIA Device Bit Rate** field, type the baud of the CDR device that is connected to the Electronic Industries Association (EIA) port.

    The valid bauds for this field are:
    - 300
    - 1200
    - 2400
    - 4800

- 9600

Note:

The system displays this field only if either the **Primary Output Format** field or the **Secondary Output Format** field is set to eia, and then only for a DEFINITY SI.

12. In the **Inc Attd Call Record** field, perform one of the following actions:
    - Type `y` if you want the system to generate separate records of the attendant portions of incoming calls that the attendant transfers or conferences.
    - Type `n` if you do not want the system to generate separate records of the attendant portions of incoming calls that the attendant transfers or conferences.

    Note that the system displays this field only when the **Inc Trk Call Splitting** field is set to `y`.
13. In the **Interworking Feat-flag** field, perform one of the following actions:
    - Type `y` if you want the system to record, in the **Feature Flag** field of a CDR record, that a call is an interworked outgoing ISDN call.

      An interworked call is a call that passes through more than one ISDN node.
    - Type `n` if you want the system to record, in the **Feature Flag** field of a CDR record, that there is no answer supervision for interworked calls.
14. In the **Intra-Switch CDR** field, perform one of the following actions:
    - Type `y` if you want the system to record calls within the server. If you type `y`, you must administer the Intraswitch CDR screen to specify the extensions that you want the system to monitor.
    - Type `n` if you do not want the system to record calls within the server.
15. In the **Modified Circuit ID Display** field, perform one of the following actions:
    - Type `y` if you want the system to display the circuit ID in the actual format of 100's, 10's units, for example, if you want the system to display circuit ID 123 as 123. Verify that the output device of your system can accept this format.
    - Type `n` to display the circuit ID in its default format (10's, units, 100's). For example, the system displays circuit ID 123 as 231.

      The information in the **Modified Circuit ID Display** field pertains to the following CDR output formats:

      - Printer
      - TELESEER
      - 59-character

The **Node Number (Local PBX ID)** field is a display-only field that is set to the distributed communications system (DCS) switch node number in a network of switches.

16. In the **Outg Attd Call Record** field, perform one of the following actions:
    - Type `y` if you want the system to generate separate records of the attendant portions of outgoing calls that the attendant transfers or conferences.
    - Type `n` if you do not want the system to generate separate records of the attendant portions of outgoing calls that the attendant transfers or conferences.

      Note that the system displays this field only when the **Outg Trk Call Splitting** field is set to y.
17. In the **Outg Trk Call Splitting** field, perform one of the following actions:
    - Type `y` if you want the system to create separate records for each portion of an outgoing call that is transferred or conferenced.
    - Type `n` if you do not want the system to create separate records for each portion of an outgoing call that is transferred or conferenced.
18. In the **Primary Output Endpoint** field, perform one of the following actions:
    - Type `eia` if the system uses the EIA port to connect the CDR device. This option is invalid for DEFINITY R systems.
    - Type the extension of the data module that links the primary output device to the server.
    - Type `CDR1` if the CDR device connects over a TCP/IP link, and the TCP/IP link is defined as CDR1 on the IP Services screen.
    - Type `CDR2` if the CDR device connects over a TCP/IP link, and the TCP/IP link is defined as CDR2 on the IP Services screen.
19. In the **Primary Output Format** field, perform one of the following actions:
    - Type `customized` if you do not want to use the standard CDR record formats. If you use a customized record format, your system must have call accounting software that is also customized to receive the customized records. Talk with your call accounting vendor before you select this option.
    - Type `printer` if you want the system to send the CDR record formats to a printer instead of to a record collection system or to a call accounting system.
    - Type the standard record format that you want to use on your system. The valid standard record formats are:
      - 59-char
      - expanded
      - lsu
      - lsu-expand
      - int-direct
      - int-isdn
      - int-process

- TELESEER
- unformatted

The standard record format that you choose must be compatible with the call accounting software on your system. To ensure that the standard record format that you choose is compatible with your call accounting system, talk with your vendor or see the call accounting system documentation.

20. In the **Privacy - Digits to Hide** field, type the number of dialed number digits that you want the system to hide for an extension with the **CDR Privacy** field on the Station record that is set to y.

    The valid entries for the **Privacy - Digits to Hide** field are 0 through 7.

    The system hides the dialed digits from right to left. If you type 4 in the **Privacy - Digits to Hide** field, and the user dials 5551234, the system records the dialed number as 555.

21. In the **Record Agent ID on Incoming** field, perform one of the following actions:

    - Type `y` if you want the system to record the login ID of the EAS agent in the **Dialed Number** field of the CDR record.
    - Type `n` if you want the system to record the physical extension in the **Dialed Number** field of the CDR record.

    The system displays the **Record Agent ID on Incoming** field only if the **Expert Agent Selection (EAS)** field on the Optional Features screen is set to y.

    You cannot use both the **Called VDN** field and the **Agent Login ID Instead of Group or Member** field. Only one of these fields can be set to y.

22. In the **Record Agent ID on Outgoing** field, perform one of the following actions:

    - Type `y` if you want the system to record the login ID of the EAS agent in the **Calling Number** field of the CDR record.
    - Type `n` if you want the system to record the physical extension in the **Calling Number** field of the CDR record.

    The system displays the **Record Agent ID on Outgoing** field only if the **Expert Agent Selection (EAS)** field on the Optional Features screen is set to y.

23. In the **Record Call-Assoc TSC** field, perform one of the following actions:

    - Type `y` if you want the system to generate records for call-associated temporary signaling connections.

      Consider the capacity of your call collection device before you decide to generate records for call-associated noncall-associated/temporary-signaling connection (TSCs).
    - Type `n` if you do not want the system to generate records for call-associated TSCs.

24. In the **Record Called Vector Directory Number Instead of Group or Member** field, perform one of the following actions:

    - Type `y` if you want the system to record the Vector Directory Number (VDN) in the **Dialed Number** field of the CDR record for calls that the system routes to a hunt group

because of a vector. If the system routes a call through more that one VDN, the system records the first VDN in the **Dialed Number** field of the CDR record

- Type `n` if you want the system to record the group number or the member number in the **Dialed Number** field of the CDR record for calls that the system routes to a hunt group because of a vector.

  You cannot use both the **Called VDN** field and the **Agent Login ID Instead of Group or Member** field. Only one of these fields can be set to y.

25. In the **Record Non-Call-Assoc TSC** field, perform one of the following actions:
    - Type `y` if you want the system to create records for noncall-associated temporary signaling connections.

      Consider the capacity of your call collection device before you decide to generate records for call-associated TSCs.
    - Type `n` if you do not want the system to generate records for noncall-associated TSCs.

      A TSC is a virtual connection that is established within an ISDN D-channel. For more information, see the DEFINITY® Communications System Generic 2.2 and Generic 3 V2 DS1/CEPT1/ISDN PRI Reference.
26. In the **Record Outgoing Calls Only** field, perform one of the following actions:
    - Type `y` if you want the system to record only outgoing calls.
    - Type `n` if you want the system to record incoming and outgoing calls.
27. In the **Remove # From Called Number** field, perform one of the following actions:
    - Type `y` if you want the system remove the pound sign (#) or the letter E from the **Dialed Number** field of the call detail record.

      Verify that your output device can accept this format.
    - Type `n` if you want the system to record the trailing pound sign (#) or the letter E in the **Dialed Number** field whenever interdigit time out occurs or users dial the pound sign # to indicate the end of a dialed string.
28. In the **Secondary Output Endpoint** field, perform one of the following actions:
    - Type `eia` if the system uses the EIA port to connect the CDR device. This option is invalid for DEFINITY R systems.
    - Type the extension of the data module that links the primary output device to the server.
    - Type `CDR1` if the CDR device connects over a TCP/IP link, and the TCP/IP link is defined as CDR1 on the IP Services screen.

    The system displays the **Secondary Output Endpoint** field when the you administer the **Secondary Output Format** field.

29. In the **Secondary Output Format** field, type the formats that you want your system to use for a secondary output device. The valid formats for a secondary out device are:

    - customized
    - int-direct
    - int-process
    - lsu
    - unformatted

    Caution:

    Ensure that only qualified service personnel administer a secondary output device. This option can cause loss of data when the buffer contains large amounts of data.

30. In the **Suppress CDR for Ineffective Call Attempts** field, perform one of the following actions:

    - Type `y` if you want the system to ignore ineffective call attempts. Perform this action if you have limited storage space for CDR records and the CDR records often overrun the buffer.
    - Type `n` if you want the system to record ineffective call attempts.

      Ineffective call attempt information shows you how often your users cannot place outgoing calls, or if numerous incoming calls are incomplete. You can also use the information to document attempts to contact a client when you use ISDN trunks.

    Your system requires more space for records if the system records ineffective call attempts than if the system does not record ineffective call attempts. Ineffective call attempts are calls that the system blocks because:

    - The user has insufficient calling privileges.
    - All the outgoing trunks are busy.
    - Incoming or outgoing trunks are unavailable because of trunk usage allocation for ISDN Call-by-Call Service Selection trunks.
    - Incoming calls have an network-specific facility (NSF) mismatch.
    - A cause value is provided for ISDN calls that are incomplete at the far end.

    The system record the ineffective call attempt as condition code E.

    Note:

    Even when the **Suppress CDR for Ineffective Call Attempts** field is set to `y`, it is possible to generate a CDR record for an outgoing trunk call if the **Answer Supervision Timeout** field on the Trunk Group screen for the outgoing trunk is administered to a small number (something generally less than 5 or 6). This is because when the Answer Supervision by Timeout feature is active and the timer expires,

the server treats that call as an effective call, and therefore creates a CDR record regardless of the state of the **Suppress CDR for Ineffective Call Attempts** field.

31. In the **Use Enhanced Formats** field, perform one of the following actions:
    - Type `y` if you want to use the enhanced version of the specified primary output format in your system. You cannot use enhanced formats and ISDN formats at the same time.
    - Type `n` if you do not want to use the enhanced version of the specified primary output format.

    The enhanced formats provide additional information about the time a call is in a queue and about ISDN call charges. The **Use Enhanced Formats** field pertains to following output formats:
    - Expanded
    - TELESEER
    - Lsu
    - Printer
    - Unformatted
32. In the Use **ISDN Layouts** field, perform one of the following actions:
    - Type `y` to use the ISDN version of the specified primary output format. You cannot use ISDN formats and enhanced formats at the same time.
    - Type `n` if you do not want to use the ISDN version of the specified primary output format.

    The ISDN formats provide more accurate information about the IXC and the ISDN network services that are used for a call. The **Use ISDN Layouts** field pertains to the following output formats:
    - Lsu
    - Printer
    - Any format with an ISDN layout, such as TELESEER
33. Click **Next** to see the second page of the CDR System Parameters screen.

    Note:

    The system displays this second CDR System Parameters screen only if the **Primary Record Format** field is set to customized.
34. In the **Data Item** field, type the data items in the order that you want the items to appear in the customized CDR record.

    You must include at least three fields on this CDR System Parameters screen if you want to have a customized CDR record. The first field can be any field that you choose from the table on page 467. The last two field items in a record must be **line-feed** and **return**, in that order.

Table 64: Valid data item entries

Data item	Length	Data item	Length
acct-code	15	ins	3
attd-console	2	isdn-cc	11
auth-code	7	ixc-code	4
bandwidth	2	ma-uui	1
bcc	1	node-num	2
calling-num	15	null	1
clg-pty-cat	2	out-crt-id	3
clg-num/in-tac	10	ppm	5
code-dial	4	res-flag	1
code-used	4	return	1
cond-code	1	sec-dur	5
date	6	space	1
dialed-num	23	time	4
duration	4	tsc_ct	4
feat-flag	1	tsc_flag	1
frl	1	vdn	1
in-crt-id	3		
in-trk-code	4		
line-feed	1		

35. In the **Length** field, type the maximum length of each data item, if the length of the data item differs from the default length.

    You must type `6` for the length of any date field to ensure proper output.

    In some cases, the system enforces a default field length.

    The **Record Length** field is a display-only field that contains the sum of all the numbers that you type in all the of the Length fields. If you change a **Length** field, the system automatically changes the number in the **Record Length** field.

36. Press `Enter` to save your changes.

Administering CDR for a trunk group

Procedure

1. Type `change trunk-group` *n*, where *n* is the number of the trunk group for which you want to administer CDR. Press `Enter`.
2. On the Trunk Group screen, click **Next** until you see the **Answer Supervision Timeout** field.

3. In the **Answer Supervision Timeout** field, perform one of the following actions:
   - If the **Receive Answer Supervision** field is set to n, type the number of seconds that you want the system to wait, before the system acts as if answer supervision was received from the far end.

     The system uses the timing information for outgoing and two-way trunks. For a cut-through operation, the system starts tracking the time after the system sends each outgoing digit. The system stops tracking the time after the far end sends answer supervision. If the timer expires, the system acts as if answer supervision was received. With a slenderized operation, the system starts tracking the time after the system sends the last collected digit.
   - If the **Receive Answer Supervision** field is set to y, type `0`.

   Note:

   The **Answer Supervision Timeout** field does not override answer supervision sent from the network or from DS1 port circuit timers.

   To control answer supervision that is sent by DS1 firmware, you must set the **Outgoing End of Dial (sec)** field on the **Administrable Timers** section of the Trunk Group screen.
4. In the **CDR Reports** field, perform one of the following actions:
   - If you want the system to generate records for all the outgoing calls on this trunk group, type `Y`.

     If the **Record Outgoing Calls Only** field on the CDR System Parameters screen is n, incoming calls on this trunk group also generate call detail records.
   - If you do not want calls that use this trunk group to generate CDR records, type `n`.
   - If you want the system to generate both incoming and outgoing CDR records, type `r` for a ring interval. The system also generates the ring interval CDR records that the table on page 468 shows.

     Table 65: CDR ring interval records

Type	Description
Abandoned calls	The system creates a record with condition code H. Condition code H indicates the interval from the start of ringing until the call is abandoned.
Answered calls	The system creates a record with condition code G. Condition code G indicates the interval from the start of ringing until the call is answered.
Calls to busy stations	The system creates a record with condition code I. condition code I indicates a recorded interval of 0.

     For ISDN trunk groups, the **Charge Advice** field affects the CDR information. For central office (CO), direct inward and outward dialing (DIOD), foreign exchange (FX), and wide are telecommunications service (WATS) trunk groups, the **Analog PPM** field affects the CDR information.

5. In the **Disconnect Supervision-In** field, perform one of the following actions:
   - Type `y` if you want:
     - Trunk-to-trunk transfers that involve this trunk group

       If you want trunk-to-trunk transfer in your system, you must also set the **Transfer** field on the Feature-Related System Parameters screen to `y`.
     - To make the far end server or switch responsible for releasing the trunk, when the far end server sends a release signal as the calling party releases an incoming call.
     - To enhance Network Call Redirection
   - Type `n` if:
     - You do not want trunk-to-trunk transfers that involve this trunk group.
     - The far end server does not provide a release signal
     - The hardware in your system cannot recognize a release signal.
     - You prefer to use timers for disconnect supervision on incoming calls.

   The system displays the **Disconnect Supervision-In** field if the **Direction** field is set to incoming or two-way.

   If the **Direction** field is set to outgoing, the system sets the **Disconnect Supervision-In** field to n.

   The value in the **Disconnect Supervision-In** field determines whether the system receives disconnect supervision for incoming calls over this trunk group.

   Caution:

   The system disallows trunk-to-trunk transfers unless at least one party on the call can provide disconnect supervision. If you administer the **Disconnect Supervision-In** field incorrectly, you can cause trunks to become unusable until the problem is detected and the trunks are reset. For example, if a user connects two trunks through the use of the Conference feature or the Transfer feature, and a far end Avaya S8XXX server on the resulting connection does not provide disconnect supervision, the trunks are not released. The trunks are not released because the system cannot detect the end of the call. Usually, the COS in the United States provide disconnect supervision for incoming calls, but do not provide disconnect supervision for outgoing calls. Public networks in most other countries do not provide disconnect supervision for incoming calls or outgoing calls. Talk with your network services provider to determine if the public networks in your area provide disconnect supervision.
6. Press `Enter` to save your changes.

Identifying the Inter Exchange Carrier for CDR records

Procedure

1. Type `change ixc-codes`. Press `Enter`.

   The system displays the Inter-Exchange Carrier Codes screen.
2. In the **IXC Access Number** field, type the digits that the user dials, or that AAR/ARS inserts, into the outpulsed digit string so the system can access the IXC.
3. In the **IXC Name** field, type a description of the IXC.
4. In the **IXC Code Format** field, type the format for the IXC code.
5. In the **IXC Prefix** field, type the prefix for the IXC code.
6. In the **CDR Account Code Access Code** field, type the access code that a user enters before the user enters a CDR account code.
7. Press `Enter` to save your changes.

Administering CDR for the paging ports

Procedure

1. Type `change paging loudspeaker`. Press `Enter`.

   The system displays the Loudspeaker Paging screen.
2. In the **CDR** field, perform one of the following actions:
   - If you want the system to record CDR information on the paging ports, type `Y`.
   - If you do not want the system to record CDR information on the paging ports, type `N`.
3. Press `Enter` to save your changes.

Administering the Intra-Switch CDR

Procedure

1. Type `change intra-switch-cdr`. Press `Enter`.

   The system displays the Intra-Switch CDR screen.
2. In the **Assigned Members** field, type the local extensions that you want to track with intraswitch CDR.

   The number of extensions that you can track can vary.
3. Press `Enter` to save your changes.

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.

Related links

Creating a new CDR user account on page 471
Administering Survivable CDR for the main server on page 472
Administering Survivable CDR for a Survivable Remote or Survivable Core Server on page 473

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 472 in each field.

Table 66: 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
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.

End-user procedures for Call Detail Recording

End-users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Associating a CDR account code with a call

Procedure

1. Dial the CDR account code access code that you assigned.
2. Dial an account code.
3. Dial a trunk access code (TAC) or an access code.
4. Dial the telephone number.

Considerations for Call Detail Recording

This section provides information about how the Call Detail Recording (CDR) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Detail Recording under all conditions. The following considerations apply to Call Detail Recording:

- Date and Time

  If you do not administer the time of day in your system, the software does not generate CDR records.

  If a call is in progress while you change the time of day information, the system does not record the duration of the call in the CDR record. Instead, the system records the numeric sequence 9999 in the CDR record. This sequence indicates that the call was in progress when you changed the time of day information.

- Dial plan

  If the dial plan in your system supports 6-digit or 7-digit extensions, only the formats that already support calling numbers that are longer than 7 digits support 6-digit or 7-digit extensions. Such numbers include expanded, unformatted, customized, and international ISDN calling numbers.

  All other calling number formats send only 5 digits. If the calling number is a 6-digit or a 7-digit extension, the system sends only the last 5 digits.

The following information applies to the port that the secondary CDR output device uses:

- You can use the following record types for the secondary output:
  - LSU

  - Int-Direct
  - Int-Process
  - Unformatted

- If the system cannot send records to the primary CDR output device, the system discontinues sending records to the secondary port for 2 minutes. The secondary port must operate at the highest possible speed to prevent the loss of information.
- If the output buffer is full, the system busies out the secondary port for 2 minutes. This action makes system resources available to send data to the primary CDR port before the data is lost. The system continues to busy out the secondary port for 2-minute intervals until fewer than 400 records, or 1800 records for Release 5r and later, remain in the buffer.
- When QSIG Advice of Charge is set to receive charging information during a call, message activity is increased on the signaling channel, which has an impact on maximum call capacity.

Interactions for Call Detail Recording

This section provides information about how the Call Detail Recording (CDR) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Call Detail Recording in any feature configuration.

Abbreviated Dialing

When a user uses either Abbreviated Dialing or a Facility Busy Indicator button to place a call, all the outpulsed digits appear on the record.

Answer Detection

CDR starts recording call duration at the time that the call classifier detects the answer.

Answer Detection provides more accurate call records where tone detection is possible, and Network Answer Supervision is not received.

Attendant Console

If an attendant-assisted call uses an outgoing trunk, the system records the primary extension of the user who requests the attendant service as the calling number in the CDR record. The system records the primary extension of the user, even if the attendant dialed an outside number.

Condition code 1 indicates an attendant assisted the call.

If the attendant allows through dialing, the system records the primary extension of the user who dialed the number as the calling party. Condition code 1 indicates that an attendant extended a trunk access code (TAC). Condition code 7 indicates that an attendant extended a Feature Access Code (FAC).

If Incoming or Outgoing Attendant Call Record is enabled, the system produces a separate record for the attendant portion of incoming or outgoing calls that the attendant transfers.

With attendant-assisted calls that require an account code, enter the account code before the TAC.

If the attendant redirects an incoming call to an extension, the attendant can dial an account code before the attendant dials the extension number.

There are no intraswitch-optioned attendant calls. However, the system generates intraswitch records for an intraswitch-optioned extension call to an the attendant or for a call from the attendant to an intraswitch-optioned extension. In the case of an attendant-assisted call that involves an intraswitch extension, the system records the extension of the user who called the attendant as the dialing number. The system records the extension to which the attendant extended the call as the dialed number. In this case, the record has condition code 0.

Avaya Aura® Messaging

The following example describes CDR for remote Avaya Aura® Messaging in a QSIG or Avaya Aura® (SIP) network. If station A on node 1 forwards calls to Avaya Aura® Messaging on node 2, each switch produces a call record. The record from node 1 contains A as the dialed number. The record from node 2 contains Avaya Aura® Messaging as the dialed number.

If the calling number is on a different switch within the QSIP or SIP network, or the call comes in over ISDN, the system records the:

- The actual calling number in the **Calling Number** field
- The TAC of the trunk that brings the call into the local switch in the **Incoming Trunk Access Code** field of 24-word records

  If the system uses an outgoing trunk when a user forwards, transfers, or conferences an incoming call, the system generates two separate CDR records. The system generates a record for incoming usage, and a record for outgoing trunk usage. The system records Avaya Aura® Messaging as the calling number in the outgoing trunk usage record

  If Incoming Trunk Call Splitting is enabled, and Transfer out of Voice Mail is used, CDR generates two records. The first record contains Avaya Aura® Messaging, the second record contains the transferred-to party.

Authorization Codes

The system records authorization codes in CDR records as follows:

- The account codes do not exceed 5 digits in length for non-ISDN formats and ISDN LSU formats
- The account codes do not exceed 4 digits in length for enhanced LSU formats

  The system does not record authorization codes in the 59-character CDR International Processing and International Direct records.

Automatic Selection of Direct Inward Dialing (DID) Numbers

If the system records an incoming call, the system records the DID extension number, not the room extension number.

Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS)

For ARS calls, the system records the:

- Calls made through ARS
- Calling extension number
- Facilities restriction level (FRL) of the calling extension

- Called number
- TAC of the trunk group that is used for the ARS call
- Time of call completion
- Call duration
- Interexchange carrier (IXC) code, if any

The system does not generate a CDR record if CDR is suppressed for the trunk group that ARS uses.

If CDR is not suppressed, the system generates condition code 7. The system records the following information:

- The ARS access code in the **Access Coded Dialed** field.
- The TAC for the trunk group that the call used in the **Access Code Used** field.

If an AAR call is placed to a busy trunk group, and CDR is suppressed for that trunk group, the user hears the reorder tone, and the CDR record shows an ineffective call attempt.

If an ARS call is an attendant-assisted call, the CDR record shows the call with condition code 7 instead of condition code of 1. Condition code 7 indicates an ARS call. Condition code 1 indicates an attendant-assisted call. The system generates these condition codes, because CDR is not notified until after the trunk is seized and, in this case, the trunk is not seized until the user dials the number.

With the Forced Entry of Account Codes (FEAC) capability, the system does not use the class of service (COR) of the trunk group to determine if the user must enter an account code, if the system uses ARS to access the trunk.

Automatic Callback

When the Automatic Callback feature is used for an intraswitch call, the system does not generate a CDR record for the first call attempt, nor for the ringback. However, if intraswitch is enabled for either the calling user or the called user, the system generates a CDR record of the call, if the called user answers and completes the call.

Automatic Circuit Assurance (ACA)

ACA calls generate intraswitch CDR records if CDR monitors the terminating extension. The originating extension for ACA calls cannot be administered for intraswitch monitoring.

Automatic Wakeup

The system does not generate CDR intraswitch records for wake-up calls.

Bridged Call Appearance

The system does not record CDR information about the user who bridges onto a call. Instead, the system records the number that a user dialed in the **Dialed Number** field of the CDR record. The system records the duration of the call when the last party drops off the call.

If the user originates a call over a bridged appearance, the call record contains the calling number of the bridged appearance extension, and not the extension number of the original, calling station.

Busy Verification of Terminals and Trunks

Attendants and users do not need to enter an account code to make a busy verification.

Call-by-Call Service Selection

When the system successfully makes a call on a Call-by-Call Service Selection trunk, the system translates the network-specific facility that the system uses for the call into an ISDN network service (INS) number. The system records the INS number in the **INS** field of the CDR record.

If the system is unsuccessful in making a call on a Call-by-Call Service Selection trunk because of an administered trunk usage allocation plan, the system records the INS number in the **INS** field of the CDR Record with condition code E.

CallVisor Adjunct-Switch Application Interface (ASAI)

Call classification competes with CallVisor ASAI switch-classified calls for ports on the call classifier media module. Answer Detection sends a report of a connect event to ASAI.

Call Coverage

If the system does not route a call to an off-network coverage point, the system records the extension number that the calling user dials as the dialed number when a user answers an incoming call or an intraswitch call at a covering extension.

If the system routes a call to an off-network coverage point, the system records the number at the off-network location as the dialed number. The system records the extension that has the off-network location in its coverage path as the calling number.

Call Forwarding All Calls

If the system does not forward a call to an off-network location, the system records the number that the user dials as the dialed number.

If the system forwards a call to an off-network location, the system records the number of the off-network location as the dialed number. The system records the extension from which the call was forwarded as the calling number.

The system generates one CDR record for a forwarded intraswitch call. The dialed number in the record is the extension that the calling user dialed.

The system generates two CDR records for a trunk call to a station that the system forwards to another trunk. The first record shows an incoming trunk call to the station. The second record shows an outgoing trunk call from the station.

With the FEAC capability, the system cannot forward to a destination at which a user must enter an account code.

Call Park

When a user parks an incoming call or an intraswitch call, the system records the extension of the user as the dialed number in the CDR record. The system records the entire time that the incoming trunk is busy as the duration of the incoming call. The system records the time that the call started until the call ends as the call duration for an intraswitch call.

Call Pickup

The system records the number that the user dials as the dialed number when a member of a pickup group answers an incoming call or an intraswitch call.

Call Prompting

Call classification competes with Call Prompting for ports on the call classifier media module.

Call Vectoring

You can administer CDR so the system records the vector directory number (VDN) extension instead of the extension of the Hunt Group or of the member. If you administer CDR so the system records the VDN extension, you override the Calls to Hunt Group - Record option of CDR for incoming call vectoring calls.

Outgoing vector calls generate ordinary outgoing CDR records. The system records the originating extension as the calling number.

The system records the duration of the call from the time that answer supervision is returned for incoming calls to a VDN.

- If the vector returns answer supervision, and the call does not go to another extension, the system records the VDN extension as the called number in the CDR record. The vector can return answer supervision with an announcement, collect, disconnect, or wait with music command.
- If the call terminates to a hunt group, the system records the VDN, the hunt group extension, or the agent extension as the called number in the CDR record.
- If the call terminates to a trunk, CDR generates an:
  - Incoming record with the incoming TAC as the dialed number.
  - Outgoing record with the incoming TAC as the calling number and the digits that are dialed through the vector step as the dialed number.

  If you administer member extension for CDR, the system records an incoming call to the station if the system successfully routes a call to the station with the **route-to** command.

  The system does not generate ineffective call attempt records for unsuccessful Call Vectoring **route-to** commands.

  If a vector interacts with an extension or a group that has Call Forwarding All Calls active, normal Call Forwarding and CDR interactions apply.

  Some calls look like intraswitch calls. Such calls include, for example, a call for a station that is administered for intraswitch CDR to a VDN, which becomes an outgoing call on an outgoing trunk. The system does not generate instraswitch CDR records for calls that look like intraswitch calls, but that are not intraswitch calls. The system generates a record with condition code A, which indicates outgoing.

Call Waiting Termination

The system starts the call duration timer when a user answers an incoming call.

Centralized Attendant Services (CAS)

The system records the extension of the user who originates a call as the originator of a call, if a CAS attendant extends the call to the user, and CDR is unassigned to the RLT trunk group.

The system records the RLT trunk as the originator of a call, if a CAS attendant extends the call to the user and CDR is assigned to the release-link trunk (RLT) trunk group.

The system does not generate a CDR record, if a CAS attendant answers a call but does not extend the call to a user.

CO Trunks

The system records all incoming and outgoing calls on a central office (CO) trunk group, if CDR is assigned to the trunk group, and CDR is administered to record incoming calls.

Conference

The system records a conference call for CDR, if either of the following conditions is met:

- The call uses at least one trunk that is eligible for CDR, and has two or more parties
- The call has at least one party that is optioned for intraswitch CDR.

The system records condition code C for each conference call CDR record.

The system generates a separate conference call CDR record for each outgoing trunk and each incoming trunk that serves the conference call. If you enable either, the system also generates a separate record for each internal party on the call.

For the outgoing portion of a conference call that involve multiple extensions, the system records the extension of the user who requests the outside dial tone to include another participant, as the calling party.

The system records the entire time that an incoming trunk or an outgoing trunk is used for a conference call, as the duration of the call.

The system generates a separate CDR record for each trunk that is used in a trunk-to-trunk transfer. If incoming trunk call splitting (ITCS) is active, the incoming trunk record shows the duration of the entire call.

The system starts a new CDR record whenever the originator of a conference call dials a nontrunk participant, if the conference call is optioned for intraswitch CDR. For example, station 1 is optioned for intraswitch CDR and calls station 2. Station 1 includes station 3 in the conference call. Station 1 drops from the call. Station 2 or station 3 drops from the call. The system generates two CDR records with condition code C. The system generates one record from station 1 to station 2, and another record from station 1 to station 3.

The system generates one record with condition code C for each dialed intraswitch conference participant, if any of the conference participants are optioned for intraswitch CDR. The system generates a record with condition code C, even if the originator of the conference is not optioned for intraswitch CDR. For example, station calls station 2, which is optioned for intraswitch CDR. Station 1 includes station 3 into the conference call. Station 1 drops from the call. Station 2 or station 3 drops from the call. The system generates one CDR record with condition code C from station 1 to station 2.

The system generates intraswitch conference call CDR records when both the calling party and the called party call drop from the call. The system records the call duration from the time that the called party answers the call until both the calling party and the called party drop from the call.

If an attendant originates a conference, the system generates CDR records only for the dialed numbers that correspond to any intraswitch optioned extensions.

Distributed Communications System DCS

The system does not pass station information throughout the DCS network for CDR records.

Direct inward dial (DID) trunks

If you administer the system to record incoming CDR information, and if you administer CDR for the trunk group, the system records all incoming calls on the DID trunk group.

Emergency Access to the Attendant

The system does not generate intraswitch CDR records for Emergency Access calls.

Expert Agent Selection (EAS)

You can assign a logical extension to an agent who can then use the logical extension to log in to a telephone. You can administer CDR so that the system records the logical extension of the agent as the called number. The system records the logical extension as the called number instead of the extension of the hunt-group or the hunt group member.

Foreign Exchange (FX) Trunks

If you want the system to generate CDR records for calls to FX trunks, you must administer your system to generate those records. You must also administer each trunk group so the system generates a CDR record for the trunk group.

Hotline Service

The system generates a CDR record of the stored number that is used on an outgoing or intraswitch Hotline call as if someone manually dialed the number.

Hunt Groups

You can administer CDR so the system records either the extension of the hunt group or the extension of the individual hunt group member as the called number.

Intercept Treatment

If the system routes an outgoing call or a tandem call to intercept treatment, the system records the number that the user dialed as the dialed number. The system also records condition code F.

Inter-PBX Attendant Calls

The table on page 481 shows the information that the system records if a user calls an Inter-PBX attendant, and the call uses a trunk group that has CDR assigned.

Table 67: Inter-PBX CDR information

CDR data field	Value
Condition Code	A
Access Code Dialed	Blank
Access Code Used	The TAC of the trunk that the call used
Dialed Digits	The Inter-PBX attendant access code

ISDN

The system sends an indication to the CDR device when the system receives a true answer supervision.

The system creates a CDR record each time that the system networks an ISDN call. In this case, the answer supervision information that the system records might not be accurate. If you use unformatted or expanded record formats, the CDR record displays the station identification number (SID) or the automatic number identification (ANI), if the SID or ANI is sent.

Last Number Dialed

The system stores the CDR access code and the account code that the user dials as part of the Last Number Dialed. However, some digits might be lost, because of the limit on the number of digits that can be stored for the Last Number Dialed feature.

Manual Originating Line Service

If an attendant establishes an outgoing call for a user, and designates the call as a Manual Originating Line call, the system generates an attendant-assisted outgoing call CDR record. The system records the extension of the user who originated the call as the calling number, and applies condition code 1.

Multiple Listed Directory Numbers (LDNs)

If the system records incoming call information, the system records the extension number or the TAC to which the attendant completes the call, as the called number of LDN calls.

If the system records incoming call information, the system records the attendant extension as the dialed number, if the call terminates at the attendant console.

You cannot administer LDNs for intraswitch CDR. However, the system generates an intraswitch CDR record for a call from an intraswitch-optioned extension to an LDN.

Night Service

The system records the extension number that is assigned to the attendants as the dialed number for night service calls.

Off-Premises Station

The system generates a CDR record for a call to an off-premises station when the:

- Call involves an outgoing or an incoming trunk call.
- Off-premises station is optioned for intraswitch CDR.
- Other terminal that is involved in the call is optioned for intraswitch CDR.

Personal Central Office Line (PCOL) trunks

If the system records incoming calls, the system records the primary extension of the user who answers the call as the called number for incoming PCOL call.

The system records an outgoing PCOL call as a call from the originating extension number through the trunk group that is associated with the PCOL.

The system records the dialed number in the **Dialed Number** field for an outgoing PCOL call. The system does not record the TAC in the **Dialed Number** field for an outgoing PCOL call.

Planned Interchange

When any planned interchange occurs, the system might record calls that end within 10 to 20 seconds after the interchange as calls that have an invalid duration. A call with an invalid duration is a call with a duration of 9:59:9, and a condition code other than 4. These call records are invalid. Deviations in the clocks between the two processors, and the short duration of the calls, cause the invalid duration.

Private Network Access

The system records Private Network Access calls, if CDR is assigned for incoming or outgoing tie trunks.

Remote Access

The system records remote access calls if Remote Access is provided on a per-trunk-group basis, and you administered CDR for those trunks. The trunk group access code in the call record is the only indication that the record is for a remote access call.

Ringback Queuing

The system records condition code 8 for an outgoing call that is in a trunk queue before the call is complete. The system does not record the time that the call is in the queue.

The system does not generate a CDR record if a call waits in a trunk queue, and the call is completed. The call is not completed successfully if the time that the call waits in the queue exceeds the wait limit for the queue, or if the calling party does not answer the callback.

Security Violation Notification (SVN)

The system generates a CDR record for a SVN call if the terminating extension is monitored. You cannot administer the originating extension for intraswitch monitoring.

Service Observing

The system does not generate CDR records for Service Observing calls.

Tandem Tie-Trunk Switching

The calling party on an incoming trunk can dial the CDR account code. The system records the TAC for the incoming trunk group in the **Calling Number** field in the CDR record. The system records the number that the user dials as the number dialed.

Temporary Bridged Appearance

A CDR record is unaffected if a second user, or subsequent user, bridges a call.

Temporary Signaling Connections (TSCs)

If you administer CDR to use ISDN layouts, the system records call-associated TSCs and TSC requests in the call record. If you administer CDR to record noncall-associated/temporary-signaling connection (NCA TSCs) and TSC requests, the system generates separate CDR records for each type of TCS. The system records the TCS data in the **TSC Flag** field and **Packet Count** field.

Tie-Trunk Access

Tie-trunk calls are recorded if CDR is administered to record the trunk group, and to record incoming calls.

Transfer

If a user originates a call on an outgoing trunk and then transfers the call to another extension, the system records the originating extension as the calling party.

If a user receives a call on an incoming trunk and then transfers the call to another extension, the system records the extension that originally received the call as the dialed number.

If a user receives an intraswitch call and then transfers the call to another extension, the system records the extension that originally received the call as the dialed number.

The system generates two CDR records if all the following conditions are met:

- Call splitting is active.

- A user receives or originates a trunk call.
- The user transfers the call to another extension

The system generates intraswitch CDR records for each call to or from an intraswitch optioned extension. For example, station A, which is intraswitch optioned, calls station B. Station A then transfers the call to station C. When either station B or station C drops, the system generates two CDR records with a condition code 0. The system generates a CDR record for a call from station A to station B, and a second record for the call from station A to station C.

The system generates intraswitch CDR transfer records when both the calling party and the called party drop from the call. The system records the call duration from the time that the called party answers the call until both the calling party and the called party drop the call.

The system generates an incoming trunk call CDR record if ITCS is enabled, and a user transfers the call to a local extension that is optioned for Intraswitch CDR. The system does not generate an intraswitch record.

When a user transfers a call to another extension, a users cannot dial an account code, unless the user has console permissions.

When a user transfers a call to a trunk, the user can dial an account code before the user dials the ARS or the TAC.

Trunk-to-Trunk Transfer

With CDR, the system processes a trunk-to-trunk transfer connection as a conference call. The system generates a separate CDR record for each trunk in the connection.

You can administer CDR so that the system records unanswered trunk calls. You can administer each trunk group so the system records unanswered calls if the calls remain unanswered for an interval that you specify.

If Incoming Trunk Call Splitting is active, the system generates a CDR record for a trunk-to-trunk transfer. The system generates a record of the incoming call, and a record of the outgoing call. The system records the duration of the outgoing call from the time that the user transfers the call until both parties drop the call. The system records the duration of the incoming call from the time that the user answers the call until both parties drop the call.

Uniform Dial Plan (UDP)

The table on page 484 shows the information that the system records if a user uses a UDP extension to call another user, and the trunk group that the call uses has CDR assigned.

Table 68: Uniform dial plan CDR information

CDR data field	Value
Condition Code	7
Access Code Dialed	Blank
Access Code Used	The TAC of the trunk that the call used
Dialed Digits	The UDP extension

VDN Return Destination

The system does not generate a CDR record for an incoming call until the originator drops from the call. The system creates a CDR record when all the following conditions are met:

- A call goes to the return-destination VDN.
- The originator has not dropped.
- Vector processing, that is the return destination VDN, routes the call to an outgoing trunk.

The system does not create a CDR record if vector processing routes a call from the return-destination VDN to an internal call. The system records only the first VDN that the caller accesses, regardless of the number of other extensions that are involved in the call.

If the system routes an incoming VDN call to a station, the system includes the station in the CDR record. If the system routes an incoming VDN call to an outgoing trunk, the system includes the VDN in the CDR record.

Interactions for QSIG Supplementary Service - Advice of Charge

The following are the interactions for the QSIG Supplementary Service - Advice of Charge feature:

Adjunct-Switch Application Interface (ASAI)

ASAI Advice of Charge and CDR may both receive charge information from the network about the same trunk.

Call Detail Recording

- When the **Charge Advice** field is set to either end-on-request or during-on-request CDR records charge advice and displays it on the user's terminal.
- For CDR Call Splitting to work properly, QSIG Advice of Charge must be set to receive charge information during the call. (Call Splitting applies to calls with endpoints within a Communication Manager system as parties of a call that also have a trunk endpoint in the call for which CDR is enabled.)
- If Call Splitting is enabled, the CDR record associated with the final party on an outgoing call contains the ISDN call charge for the entire call, since no charge advice data is available until the final party drops off the call. The ISDN call charge in all earlier CDR records is 0 (zero). However, the Elapsed Time in the CDR records is correct and can be used to allocate the call charge among the parties on the call.
- If Call Splitting is disabled, the CDR record associated with the party that made the initial outgoing call contains the ISDN call charge for the entire call.
- For calls diverted to another switch, if Call Splitting is enabled when an outgoing call is transferred, a CDR record is issued for the initial portion of the call, and the **ISDN Call Charge** field reports the Advice of Charge information received thus far. Subsequent Advice of Charge information received from the network for the outgoing call is not sent to the switch to which the call is diverted.

In cases in which the CDR adjunct is to collect information at a switch other than the one directly connected to the PSTN, all switches in the PTN must be upgraded to be able to transport the QSIG messages at the served user switch.

Call Transfer

An originating user can request a call transfer during a call in which Advice of Charge has been invoked. In this scenario:

- Communication Manager, as an outgoing gateway, does not provide charge data to the transferring or transferred-to switch at the end of the call.
- The gateway may or may not know the call is transferred unless it receives an invocation for an additional charge request after Call Transfer from the transferred-to switch. If an invocation is received, then only interim charge information can be sent to the originating switch.
- If the interim charge information is used on the PSTN side, but the call continues after the transfer is complete, then final charge information is not interworked into the PTN to any switch. If the call continues on the PSTN side, any charge information received from the PSTN is not interworked into the PTN.

Charge Advice Display

The charge information can additionally be displayed at the served user’s calling endpoint, either automatically or manually.

Chapter 55: Call Forwarding

Use the Call Forwarding feature to redirect calls to an:

- Internal extension
- Off-network number
- Attendant group

Detailed description of Call Forwarding

Call Forwarding All Calls

Users use the Call Forwarding All Calls capability to redirect any incoming calls to another destination. You can restrict access to the Call Forwarding All Calls capability to specific users.

A user cannot have both the Call Forwarding All Calls capability and the Call Forward Busy/Don't Answer capability active at the same time.

The system forwards a call only once. For example, assume that extension A designates extension B as its forwarded-to destination, and that extension B designates extension C as its forwarded-to destination. When someone calls extension A, the system first attempts to ring the call at extension A. If the system is unable to ring the call at extension A, the system attempts to ring the call at extension B. If the system is unable to ring the call at extension B, the system redirects the call to the coverage path of extension A, if a coverage path is available at extension A, and if the coverage criteria of extension A are satisfied when applied at extension B. The system does not forward the call to extension C under any circumstances.

The system can forward an unlimited number of calls simultaneously.

When a call gets forwarded, the recipient of the forwarded call can view the forwarding party extension along with the administered numbering plan prefix. The prefix helps to identify the location of the called party.

Call Forwarding All Calls and FAC

Users use a Feature Access Code (FAC) or a **Call Forward-All feature** button to activate or deactivate Call Forwarding All Calls for their own telephone. Virtual extension users cannot

activate or deactivate Call Forwarding All Calls. Users can activate or deactivate the Call Forwarding All Calls feature for the following entities:

- Another extension
- A virtual extension
- An Automatic Call Distribution (ACD) split

Call Forwarding and attendants

The attendant cannot have a **Call Forwarding** button.

The system does not forward calls to attendants. However the system does forward calls to an attendant group.

Only the attendant, or a telephone user with console permission, can activate the Call Forwarding All Calls capability for the following entities:

- A terminating extension group (TEG)
- A direct department calling (DDC) hunt group
- A uniform call distribution (UCD) hunt group
- Data modules

Attendants and users cannot activate or deactivate the Call Forwarding All Calls capability for a vector-controlled split under any circumstances.

Call Forward Busy/Don’t Answer

Users use the Call Forward Busy/Don’t Answer capability to redirect incoming calls to another destination when the user:

- Is busy on a call

  If the user is busy on a call, the system immediately forwards the call. The system does not cause the telephone to ring before the system forwards the call to another destination.

- Does not answer the call within the allowed time interval

  If the user does not answer the call, the telephone rings for the allowed time interval. At the end of the interval, the system forwards the call to another destination.

You can restrict access to the Call Forward Busy/Don’t Answer capability to specific users.

A user cannot have both the Call Forward Busy/Don’t Answer capability and the Call Forwarding All Calls capability active at the same time.

Users activate or deactivate the Call Forward Busy/Don’t Answer capability with an FAC or a Call Forward Busy/Don't Answer feature button. Attendants or users that have console permission can also activate or deactivate the feature for another extension with an FAC. Virtual extension users cannot activate or deactivate Call Forwarding Busy/Don’t Answer.

Call Forward Busy/Don't Answer cannot be activated for calls to hunt groups, data extensions, a TEG, or an Expert Agent Selection (EAS) agent.

Call Forwarding Off-Net

Users use the Call Forwarding Off-Net capability to forward calls to an off-network destination. However, you can restrict access to the Call Forwarding Off-Net capability to specific users.

If the Coverage of Calls Redirected Off-Net (CCRON) capability is enabled, and the called user has a coverage path, the system monitors a call for call progress tones. If no one answers the call at the off-network destination, or if the destination is busy, the system returns the call to the internal extension. For more information on the Call Coverage feature, see *Administering Avaya Aura® Communication Manager*.

The system can bring the call back for call-coverage processing if the coverage criteria of the principal are satisfied at the forwarded-to destination.

If the CCRON capability is enabled, but the called user does not have a coverage path, the system does not monitor a call for call progress tones. The system leaves the call at the off-network destination.

When the system redirects an incoming trunk call off the network, the system sets a timer. The timer prevents the system from redirecting the incoming trunk calls off the network until the timer either expires or is canceled. The timer prevents calls that are redirected off the network from being routed back to the original telephone number from the off-network destination. Calls that are routed back to the original telephone number in this situation effectively create a loop that seizes trunks until trunks are no longer available.

Call Forwarding Override

With the Call Forwarding Override capability, you can call, or transfer a call to a user who has the Call Forwarding feature active. Only the user who answers the forwarded call can use the Call Forwarding Override capability to transfer the call back to the called extension. For example, user A designates user B as the destination for forwarded calls. User B answers a call forwarded from the extension of user A, and uses the Call Forwarding Override capability to transfer the call back to user A.

If you enable the Call Forwarding Override capability on your system, the capability is available for all users.

Users cannot use the Call Forwarding Override capability to override a call when the system forwards a call from a data user or from a hunt group.

In Communication Manager 4.0 and earlier releases, Call Forward Override did not work if the forwarded-to party was not on the same Communication Manager server as the forwarding party. Starting in Communication Manager 5.0, this is now possible, as long as the call from the forwarded-to party provides the calling number in a format that Communication Manager can match with the forwarded-to number entered by the forwarding party. Trunk groups that can do this include ISDN-PRI, ISDN-BRI, H.323, and SIP.

Example 1: Ivan forwards his calls using UDP to extension 2346. An incoming QSIG call for Ivan arrives with the Calling Number “2346.” The call is not forwarded, but rings Ivan's phone.

Example 2: Sylvia in Germany forwards her calls to a public network number in Frankfurt using ARS to 0-069-5354341. (The leading '0' is the ARS FAC, and the second '0' is National CPN Prefix.) An incoming call for Sylvia arrives with the Calling Number “49695354341.” The “49” is recognized as the local country code and is skipped. Likewise, the ARS FAC and National CPN Prefix are recognized and skipped in the forwarded-to number. The remaining digits match, so the call is not forwarded, but rings Sylvia's phone.

Example 3: Mike in the U.S. forwards his calls to a private-network number at the Chicago office using AAR to 8-231-8592. (The leading '8' is the AAR FAC.) An incoming call for Mike arrives with the Calling Number “231-8592.” The AAR FAC is recognized and skipped in the forwarded-to number. The remaining digits match, so the call is not forwarded, but rings Mike's phone.

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

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

Notifying users when their calls are redirected

You can administer a setting to notify users that they have a capability active that might redirect their calls. For example, if call forwarding is active for a user, you can administer a setting to play a special dial tone when the user goes off hook.

Coverage for unanswered forwarded calls

You can specify that unanswered forwarded calls have call coverage treatment. The system sends an unanswered forwarded call to coverage if you:

- Enable coverage for unanswered forwarded calls for your system
- Enable call forwarding capabilities for the user
- Assign a call coverage path for the user

Security for Call Forwarding Off-Net

Users who do not have permission to make calls to an off-network destination cannot use the Call Forwarding feature to forward calls to an off-network destination.

Call Forwarding administration

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

- Enabling call coverage for unanswered forwarded calls
- Viewing user extensions that have the Call Forwarding capabilities active
- Assigning the Call Forwarding All Calls capability to a user
- Removing the Call Forwarding All Calls capability for a user
- Assigning the Call Forward Busy/Don't Answer capability to a user
- Removing the Call Forward Busy/Don't Answer capability for a user
- Assigning the Call Forwarding Off-Net capability to a user
- Removing the Call Forwarding Off-Net capability for a user
- Enabling the Call Forwarding Override capability for your system
- Disabling the Call Forwarding Override capability for your system

Related links

Enabling the Call Forwarding Override capability for your system on page 496
Disabling the Call Forwarding Override capability for your system on page 496
Removing the Call Forwarding All Calls capability for a user on page 493
Assigning the Call Forwarding All Calls capability to a user on page 493
Viewing user extensions that have the Call Forwarding capabilities active on page 492
Enabling call coverage for unanswered forwarded calls on page 492
Assigning the Call Forward Busy/Don’t Answer capability to a user on page 493
Assigning the Call Forwarding Off-Net capability to a user on page 494
Removing the Call Forwarding Off-Net capability for a user on page 496
Removing the Call Forward Busy/Don’t Answer capability for a user on page 494

Preparing to administer Call Forwarding

Procedure

1. Ensure that a class of service (COS) to use the Call Forwarding feature exists on your system.

   The Call Forwarding feature requires a COS that supports:

   - Call Fwd-All Calls
   - Call Forwarding Busy/DA
   - Restrict Call Fwd-Off Net

   For information on COS administration, see the Class of Service feature.

2. Ensure that Feature Access Codes (FACs) for Call Forwarding and Call Forward Busy/Don’t Answer are available on your system, if you want users to use an FAC for either of the capabilities.

The Call Forwarding feature requires the following FACs:

- Call Forwarding Activation All
- Call Forwarding Activation Busy/DA

For more information on FAC administration, see the Feature Access Code feature.

Screens for administering Call Forwarding

Screen Name	Purpose	Fields
Class of Service	Enable Call Forwarding capabilities for users.	• Call Fwd-All Calls • Call Forwarding Busy/DA • Restrict Call Fwd-Off Net
Feature Access Code (FAC)	Assign a FAC for the Call Forwarding capabilities.	• Call Forwarding Activation All • Call Forwarding Activation Busy/DA
Station	Assign a Class of Service (COS) that has the Call Forwarding capabilities enabled.	COS
System-Parameters Coverage/Forwarding	Enable the Call Forwarding Override capability.	• Call Forward Override • Coverage After Forwarding
System Parameters Customer-Options	Ensure that the system can forward calls to an off-network destination.	Restrict Call Forward Off Net

Enabling call coverage for unanswered forwarded calls

Procedure

1. Enter `change system-parameters coverage-forwarding`.
2. Perform one of the following actions:
   - If the **Coverage After Forwarding** field is set to y, press `Cancel`.
   - If the **Coverage After Forwarding** field is set to n:
     - Type `y` in the field.
     - Select **Enter** to save your change.

Viewing user extensions that have the Call Forwarding capabilities active

Procedure

Type `list call-forwarding`. Press `Enter`.

This system lists the extensions, with the forwarded destination, that have an active call forwarding capability.

Note:

If you have a V1, V2, or V3 system, the **list call-forwarding** command is unavailable. However, you can use the **display station** command to view the call forwarding capabilities that are active for a single user extension.

Assigning the Call Forwarding All Calls capability to a user

Procedure

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

   The system displays the Station screen.

2. In the **COS** field, type the number of a COS that has the Call Forwarding All Calls capability enabled.
3. Press `Enter` to save your change.

Removing the Call Forwarding All Calls capability for a user

Procedure

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

   The system displays the Station screen.

2. In the **COS** field, type the number of a COS that does not have the Call Forwarding All Calls capability enabled.
3. Press `Enter` to save your change.

Assigning the Call Forward Busy/Don’t Answer capability to a user

Procedure

1. Assign the Call Forward Busy/Don’t Answer ring interval for calls that the system forwards to an internal extension.
2. Assign Call Forward Busy/Don’t Answer to a user by assigning a COS with Call Forward Busy/Don’t Answer enabled.

Related links

Assigning the Call Forward Busy/Don’t Answer ring interval for internal extensions on page 493
Assigning Call Forward Busy/Don’t Answer to a user on page 494

Assigning the Call Forward Busy/Don’t Answer ring interval for internal extensions

Procedure

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

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

2. In the **Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings)** field, type the number of times that a telephone rings before the system forwards the call.

   The system uses this interval when the Call Forward Busy/Don't Answer capability is active for a user.

3. Press `Enter` to save your change.

Assigning Call Forward Busy/Don't Answer to a user

Procedure

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

   The system displays the Station screen.

2. In the **COS** field, type the number of a COS that has the Call Forward Busy/Don't Answer capability enabled.

3. Press `Enter` to save your change.

Removing the Call Forward Busy/Don't Answer capability for a user

Procedure

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

   The system displays the Station screen.

2. In the **COS** field, type the number of a COS that does not have the Call Forward Busy/Don't Answer capability enabled.

3. Press `Enter` to save your change.

Assigning the Call Forwarding Off-Net capability to a user

Before you begin

1. On the Optional Features screen, verify that the **Restrict Call Forward Off Net** field is set to Y. To view the screen, type `display system-parameters customer-options`. Press `Enter`.

   If you set the **Restrict Call Forward Off Net** field to n, the system will not support the Call Forwarding Off-Net capability. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to assigning Call Forwarding Off-Net capability to a user, or to open a service request.

   For a complete description of the System Parameters Customer-Options screen, see *Administering Avaya Aura® Communication Manager* for more information.

Procedure

1. Enable Call Forwarding Off-Net for the system.
2. Assign a ring interval for the Off-Net Call Forward Busy/Don’t Answer capability.
3. Assign Call Forwarding Off-Net to a user by assigning a COS with Call Forwarding Off-Net enabled.

Related links

Enabling Call Forwarding Off-Net on page 495
Assigning the Off-Net Call Forward Busy/Don’t Answer ring interval on page 495
Assigning Call Forwarding Off Net to a user on page 495

Enabling Call Forwarding Off-Net

Procedure

1. Type `change system-parameters coverage-forwarding`. Press `Enter`.
2. On the System Parameters Call Coverage/Call Forwarding screen, click **next** until you see the **Coverage Of Calls Redirected Off-Net Enabled** field.
3. Set the **Coverage Of Calls Redirected Off-Net Enabled** field to `y`.
4. Press `Enter` to save your change.

Assigning the Off-Net Call Forward Busy/Don’t Answer ring interval

Procedure

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

   The system displays the System Parameters Call Coverage/Call Forwarding screen.
2. In the **Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings)** field, type the number of times that a telephone rings before the system forwards the call.

   The system uses this interval when the Call Forward Busy/Don’t Answer capability is active for a user, and the forwarded-to number is an off-network destination.
3. Press `Enter` to save your change.

Assigning Call Forwarding Off Net to a user

Procedure

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

   The system displays the **Station** screen.
2. In the **COS** field, type the number of a COS that has the Call Forwarding Off-Net capability enabled.
3. Press `Enter` to save your change.

Removing the Call Forwarding Off-Net capability for a user

Procedure

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

   The system displays the Station screen.

2. In the **COS** field, type the number of a COS that does not have the Call Forwarding Off-Net capability enabled.
3. Press `Enter` to save your change.

Enabling the Call Forwarding Override capability for your system

Procedure

1. Type `change system-parameters coverage-forwarding`. Press `Enter`.
2. On the System Parameters Call Coverage/Call Forwarding screen, set the **Call Forward Override** field to y.
3. Press `Enter` to save the changes.

Disabling the Call Forwarding Override capability for your system

Procedure

1. Enter `change system-parameters coverage-forwarding`.
2. On the System Parameters Call Coverage/Call Forwarding screen, set the **Call Forward Override** field to `n`.
3. Select **Enter** to save your changes.

End-user procedures for Call Forwarding

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Changing the Call Forwarding All Calls destination from an internal telephone

Procedure

1. Go off hook.
2. Dial the Feature Access Code (FAC) for Call Forwarding Activation All or press the **Call Forwarding Activation All** feature button.
3. Listen for a dial tone.

4. Dial the extension number of the destination.
5. Disconnect the telephone after you hear the three-beep tone.

Changing the Call Forward Busy/Don’t Answer destination from an internal telephone

Procedure

1. Go off hook.
2. Dial the FAC for Call Forward Busy/Don’t Answer or press the **Call Forwarding/Busy Don’t Answer** feature button.
3. Listen for a dial tone.
4. Dial the extension number of the destination.
5. Disconnect the telephone after you hear the three-beep tone.

Changing the forwarding destination when a user is at an off-network location

Procedure

1. Go off hook.
2. Dial the telecommuting extension number.
3. Dial the FAC for Extended Call Forward Activate All feature or press their **Call Forwarding Activation All** feature button.
4. Listen for a dial tone.
5. Dial the extension number and press #.
6. Dial the security code and press #.
7. Listen for a dial tone.
8. Dial the extension of the destination.

   Use no more than 18 digits when you enter your off-network call forwarding destination telephone number. Include the FAC for Automatic Alternate Routing (AAR) or Automatic Route Selection (ARS) or the Trunk Access Code (TAC) among the 18 digits. Do not include the pound key (#) that you use to terminate a forwarded-to number among the 18 digits. For more information on the AAR and ARS features, see *Administering Avaya Aura® Communication Manager*.
9. Disconnect the telephone after you hear the three-beep tone that the system generates to confirm the change.

Changing the Call Forward Busy/Don’t Answer destination when a user is at an off-network location

Procedure

1. Go off hook.
2. Dial the telecommuting extension number.
3. Dial the FAC for Extended Call Forward Activate Busy/Don’t Answer or press the **Call Forward Activate Busy/Don’t Answer** feature button.
4. Listen for a dial tone.
5. Dial the extension number and press #.
6. Dials the security code and press #.
7. Listen for a dial tone.
8. Dial the extension of the destination.

   Use no more than 18 digits when you enter your off-network call forwarding destination telephone number. You must include the FAC for Automatic Alternate Routing (AAR) or Automatic Route Selection (ARS) or the Trunk Access Code (TAC) among the 18 digits. Do not include the pound key (#) that you use to terminate a forwarded-to number among the 18 digits. For more information on the AAR and ARS features, see *Administering Avaya Aura® Communication Manager*.
9. Disconnect the telephone after they hear the three-beep tone that the system generates to confirm the change.

Call Log Enhancements

Log Forwarded Calls option

The Log Forwarded Calls operation creates missed call log entry for calls that are redirected by a forwarding feature.

Missed call log entry for a redirected call shows the forwarding icon instead of the missed call icon in the display. So the user knows that the missed call is redirected and might have been answered already by another user.

The Log Forwarded Calls option applies to the following redirecting features:

- Call-Forward
- Enhanced Call Forward
- Coverage
- Goto-Cover

- Send-all-calls

Note:

The Log Forwarded Calls feature is available with Communication Manager Release 5.2 or later, firmware version 3.0 and higher. It is available for 96xx and 96x1 H.323 IP series telephone only.

Administration of the Log Forwarded Calls option is only possible through the LOGUNSEEN parameter in the phone firmware settings file. With the setting of this parameter the logging of forwarded calls can be switched on and off.

Users wanting to have all calls logged and those not wanting to have the forwarded calls logged, the settings file of the firmware provides a new parameter for Log Forwarded Calls. The default setting is No Logging Of Forwarded Calls, because this is close to the current call log handling. The setting for logging of forwarded calls is only handled in the telephone and not in Communication Manager switching software.

The table on page 499 shows the logging of forwarded calls with the log forwarded calls active or inactive settings parameter on the telephone. The busy/do not answer details are listed separately, even though this is one feature.

Table 69: Logging of forwarded calls

Feature	Call Forward Log	Call Log on forwarding user log fwd calls not active	Call Log on forwarding user log fwd calls active
Call-forward all	Yes	No	Missed
Enh-cfwd all	Yes	No	Missed
Send-all-calls	Yes	No	Missed
Goto-cover	Yes	No	Missed
Coverage all	No	No	No
Call-forward busy	Yes	No	Missed
Enh-cfwd busy	Yes	No	Missed
Coverage busy	No	No	Missed
Coverage DND	Yes	No	Missed
Call-forward no-ans	Yes	No	Missed
Enh-cfwd no-ans	Yes	No	Missed
Coverage no-ans	No	No	Missed
Coverage active	No	No	Missed

Important:

Users cannot activate or deactivate the Coverage All feature. It is set and activated only by an administrator and will never create call log entries. So calls that are going to coverage all are not handled as forwarded calls in the call log.

When the **Call Forward All** feature is enabled on the called party station and the called party station misses a call, the called party station does not update the call log of the calling party with the missed call information. The call log scenario is only applicable for SIP endpoints.

For example, the calling party Station is A, the called party Station is B, and Station B has the **Call Forward All** feature button enabled for Station C. If Station A calls Station B, then the call is forwarded to Station C, and Station B does not update the call log with the missed call information.

Considerations for Call Forwarding

This section provides information about how the Call Forwarding feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Forwarding under all conditions.

Call classifiers and tone plans for off-network calls

If you send calls off the network and use the Call Classifier-Detector and do not use the North American tone plan, use the System-Parameters Country-Options screen to define specific country tones.

If you use the Call Classifier-Detector and do not use the System-Parameters Country-Options screen, your system downloads the North American tone plan, regardless of your geographical location.

Save translation command

If you use the **`save translation`** command, the software saves the user call forwarding information, including destination information, to tape.

Interactions for Call Forwarding

Answer Detection

The Answer Detection feature shares call-classifier resources with the Coverage of Calls Redirected Off-Net (CCRON) capability.

Attendant Override of Diversion

If an attendant uses the Call Forwarding Override to call a user who has the Call Forwarding feature active, the system sends the call to the user telephone. The system does not forward the call to the forwarded-to destination.

Automatic Callback and Ringback Queuing

A user cannot activate Automatic Callback if the Call Forwarding feature is active at the called extension. If the user activates Automatic Callback before the Call Forwarding feature is active at the called extension, the system redirects the callback call attempt to the forwarded destination.

Bridging

The system does not terminate calls to a bridged call appearance when the Call Forward Busy/ Don’t Answer capability is active at the user extension.

Users cannot bridge onto an off-network call during the time the system is classifying the call.

Call Coverage

If the principal’s (forwarding extension) redirection criteria are met at the designated (forwarded-to) destination, the forwarded call redirects to the principal’s coverage path; the designated destination gets a temporary bridged appearance (except when it is off net), which remains active after the call is answered so that the designated extension can bridge onto the call if required. The temporary bridge appearance remains until the caller hangs up.

If coverage after forwarding is disabled for calls redirected to QSIG networks, the QSIG redirection takes precedence over the CCRON capability. However, if coverage after forwarding is enabled, CCRON takes precedence, enabling the call to be tracked back to the network to follow the coverage path.

When the Cover All Calls capability is active, and either the Call Forwarding All Calls capability or the Call Forwarding Off-Net capability is active, the system:

- Forwards incoming priority call
- Redirects all nonpriority calls according to the user coverage path
- Does not redirect non-priority calls off of the network

Call Detail Recording (CDR)

When the system forwards a call off the network:

- The CDR records the forwarded-from number.
- The system generates a CDR record only after the call is answered at the off-network destination.

  If the forced entry of account codes is required, the system does not forward calls to an off-network destination.

Call Park

When a user activates Call Forwarding, and then activates Call Park, the system parks the call at the user extension. The system does not forward the call.

When the system forwards a call, and the forwarded-to extension user parks the call, the system usually parks the call at the forwarded-to extension. The system does not usually park the call at the called extension.

Call Pickup/Directed Call Pickup

If you enable a Temporary Bridged Appearance for the Call Pickup capability, the system maintains a temporary bridged appearance when the forwarded-from user and the forwarded-to user are members of the same call pickup group.

Call Prompting

The Call Prompting feature shares call-classifier resources with the Coverage of Calls Redirected Off-Net capability.

Call Visor Adjunct Switch Application Interface (ASAI)

The Call Visor ASAI feature shares call-classifier resources with the Coverage of Calls Redirected Off-Net (CCRON) capability.

Conference

Users cannot use the Conference feature to add another user to an off-network call while the system classifies the call.

The system does not classify a call when the system routes a call to an off-network destination if any of the conference participants is on hold while the conference is initiated. The system does not classify the call even if the Coverage of Calls Redirected Off Net capability is active.

Expert Agent Selection (EAS)

Agents who are logged in at an extension, and who have EAS enabled, cannot activate or deactivate Call Forwarding. If the agent logs out of the extension, the agent can activate or deactivate Call Forwarding for the extension. If the agent logs out of the extension and the agent activates Call Forwarding for the extension, the system forwards calls that are made to the extension.

Hold

The system does not classify a call when the system routes a forwarded call to an off-network destination if any party on the call is on hold. The system does not classify the call even if the Coverage of Calls Redirected Off Net capability is active.

Intercom-Automatic

When a user presses an **Intercom-Automatic** button, and Call Forwarding is active at the user extension that is associated with that button, the system forwards the Intercom-Automatic feature along with the call. However, if the system forwards the call to an off-network destination, the system does not also forward the Intercom-Automatic feature.

Interflow

The system uses the Call Forwarding All Calls capability and the Interflow feature to redirect Automatic Call Distribution (ACD) calls to an ACD split on another system.

Intraflow

The system uses the Call Forwarding feature to route ACD calls from a split to another destination on the same switch.

Leave Word Calling (LWC)

LWC cannot be activated toward a telephone that has Call Forwarding activated. If LWC was activated before the user of the called phone activated Call Forwarding, the callback call attempt is redirected to the forwarded-to party.

Multifrequency Compelled (MFC) Signaling

MFC Signaling shares call classification resources with the Coverage of Calls Redirected Off-Net capability.

Personal Central Office Line (PCOL)

The system does not forward PCOL calls.

QSIG

If a call is forwarded over an ISDN-PRI trunk that is administered with supplementary service protocol “b” (QSIG), then additional call information might be displayed.

Send All Calls

If both Send All Calls and Call Forwarding All Calls are active at an extension, the system:

- Redirects calls to coverage immediately, if the system can do so
- Forwards other calls, such as Priority Calls

  If a user has both Send All Calls and Call Forwarding All Calls activate, calls to that extension that can immediately be redirected to coverage are redirected. However, other calls, such as Priority Calls, are forwarded to the designated extension.

  Activation of Send All Calls at the forwarded-to extension does not affect calls that are forwarded to that extension.

Temporary Bridged Appearance

The system maintains a temporary bridged appearance for calls that are ringing on the network. If the caller hangs up, or someone answers the call, the system drops the temporary bridged appearance.

The system does not maintain a temporary bridged appearance when the system forwards calls to an off-network destination.

Traffic Reports Removed

Use the list measurement tone-receiver traffic report to obtain information on port usage for the Traffic Reports Removed feature.

Transfer

Users cannot transfer a call that the system routes to an off-network destination while the system classifies the call.

Chapter 56: Call Park

Use the Call Park feature to retrieve a call that is on hold, from any other telephone within the system. For example, a user can answer a call at one extension, put the call on hold, and then retrieve the call at another extension. Or the user can answer a call at any telephone after an attendant or another user pages the user.

Detailed description of Call Park

You can set a system-wide expiration interval for parked calls. If no one answers the call before the interval expires, the system redirects the call.

The system redirects a parked call to the attendant if the **Deluxe Paging and Call Park Timeout to Originator** field on the Feature-Related System Parameters screens is set to n. The system redirects a parked call to the user who parked the call if the **Deluxe Paging and Call Park Timeout to Originator** field on the Feature-Related System Parameters screens is set to y.

If you do not administer an attendant, a night service extension, or the Night Service-Trunk Answer feature, the system ignores the expiration interval, and the call remains parked.

If two parties are connected on a parked call, a third party can create a three-way conference, if the third party answers the call before the interval expires.

The attendant console group can have common shared extensions that the attendant console group uses exclusively for the Call Park feature. The system does not assign the common shared extensions to a telephone. The system stores the common shared extensions in the system translations, and parks calls at the extensions.

The common shared extensions are particularly useful when an attendant pages a user at the request of another user. The attendant parks the calling user on a common shared extension, and announces the extension. The status lamp that is associated with the extension indicates call parked or no call parked, instead of an active or idle status.

If a user parks a call and does not disconnect after hearing the confirmation tone, the user stays connected to other parties on the call. To automatically disconnect the call, set the **Drop Parking User From The Call After Timeout** field on the Feature-related system parameters screen to y. The system then drops the parked call after the default time limit of 5 seconds if the user does not disconnect the call. You cannot change the default time limit.

In Communication Manager Release 6.0, you can administer the call unpark button on the SAT screen for SIP telephones. Starting with SIP telephone firmware 2.6, the call park button provides

a toggle functionality to park and unpark the same call, from the same telephone. For SIP telephones that do not support the toggle functionality, you can administer the call unpark button. You must administer the call unpark button whenever you need to unpark a call from a different SIP telephone than the one used to park the call.

For information on how to assign a call unpark button to a SIP telephone, see Assigning a call unpark button to a SIP telephone.

The Call Park feature in Communication Manager is different from the features provided with Call Park and Page Snap-in. For information about Call Park and Page Snap-in, see *Call Park and Page Snap-in Reference*.

Call Park administration

The following tasks are part of the Call Park feature:

- Administering Call Park Feature-Related System Parameters
- Defining common shared extensions for Call Park
- Assigning a call park button to a multiple-call appearance telephone
- Assigning a call unpark button to a SIP telephone

Related links

Administering Call Park Feature-Related System Parameters on page 506
Defining common shared extensions for Call Park on page 507
Assigning a call park button to a multiple-call appearance telephone on page 507
Assigning a call unpark button to a SIP telephone on page 507

Preparing to administer Call Park

Procedure

1. Type `change feature-access-codes`. Press `Enter`.
2. On the Feature Access Codes (FAC) screen, perform one of the following actions:
   - If the **Answer Back Access Code** field and the **Call Park Access Code** field each contain an FAC, your system already has the FACs that are necessary for the Call Pickup Feature. Press **Cancel**.
   - If either the **Answer Back Access Code** field or the **Call Park Access Code** field do not contain a FAC, type a FAC in the field. Press `Enter` to save your changes.

     For more information on the Feature Access Code feature, including how to change or deactivate an FAC, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Call Park

Screen name	Purpose	Fields
Console-Parameters	Specify the extensions where an attendant can park a call.	• Starting Extension • Count
Feature Access Code (FAC)	Define the system-wide FACs to use to park a call, and to answer a parked call.	• Answer Back Access Code • Call Park Access Code
Feature-Related System Parameters	Specify the number of minutes that the system parks a call on your system.	Call Park Timeout Interval
	Specify that the system return a call that exceeds the timeout to the originator of the call.	Deluxe Paging and Call Park Timeout to Originator
	Specifies to the system to automatically drop the parking user from the call after the timeout that is set.	Drop Parking User From the Call After Timeout
Station	Assign a call park button to a user with a multiple-call appearance telephone.	Button assignments for call park (call-park)
	Assign a call unpark button for a SIP station.	Button assignments for unpark call (call-unpk)

Administering Call Park Feature-Related System Parameters

Procedure

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

   The system displays the Feature-Related System Parameters screen.
2. In the **Call Park Timeout Interval (minutes)** field, type the number of minutes that you want the system to park a call at an extension.
3. Click **Next** until you see the **Deluxe Paging and Call Park Timeout to Originator** field.
4. In the **Deluxe Paging and Call Park Timeout to Originator?** field, perform one of the following actions:
   - If you want the system to route a parked call, that exceeds the number of minutes that you specified in the **Call Park Timeout Interval (minutes)** field, to the attendant, type `n`. The system provides n as the default entry for this field.
   - If you want the system to route a parked call, that exceeds the number of minutes that you specified in the **Call Park Timeout Interval (minutes)** field, to the originator of the call, type `y`.
5. Press `Enter` to save your changes.

Defining common shared extensions for Call Park

Procedure

1. Type `change console-parameters`. Press `Enter`.
2. On the Console Parameters screen, click **Next** until you see the **Common Shared Extensions** area.
3. In the **Starting Extension** field, type an extension at which you want the attendant to park a call.
4. In the **Count** field, type the number of extensions that you want the attendants to have available to park calls.

   The system uses the information in the **Starting Extension** field and the **Count** field to determine which extensions are available for attendants to park a call. For example, if you type `4300` in the **Starting Extension** field and you type `3` in the **Count** field, the system provides the three consecutive extensions 4300, 4301, and 4302 to park calls.
5. Press `Enter` to save your changes.

Assigning a call park button to a multiple-call appearance telephone

Procedure

1. Type `change station` *n*, where *n* is the telephone number of the extension to which you want to assign a call park button. Press `Enter`.
2. On the Station screen, click **Next** until you see the **Button Assignments** area.
3. Type `call-park` next to the number of the button that you want the user to use to park a call.
4. Press `Enter` to save your changes.

Assigning a call unpark button to a SIP telephone

Procedure

1. Type `change station` *n*, where *n* is the telephone number of the extension to which you want to assign a call unpark button. Press `Enter`.
2. On the Station screen, click **Next** until you see the **Button Assignments** area.
3. Type `call-unpk` next to the number of the button that you want the user to use to unpark a call.
4. Press `Enter` to save your changes.

Note:

DCP and H.323 IP telephones must use the answer back feature access code and the extension where the call is parked to retrieve parked calls from a station that did not park the call.

End-user procedures for Call Park

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Using Call Park from a single-line telephone

Procedure

1. Flash the switch hook.
2. Dial the Feature Access Code (FAC) for Call Park.
3. Disconnect the call.

Using Call Park from a multiple-call appearance telephone

Parking a call using the FAC

Procedure

1. Press the **transfer** button or the **conference** button.
2. Dial the FAC for Call Park.
3. Dial the extension of the telephone where you want to park the call.
4. Press the **Complete** button.

Note:

While call park using the FAC, the confirmation tone is heard by, only the party who is parking the call and a confirmation tone is heard by both the parties while **Call Unpark**.

Parking a call using the call park button

Procedure

1. Press the call park button to park a call.
2. Disconnect the call.

Note:

Pressing the call-park button sends a confirmation tone to both the parties on the call. The confirmation tone sent is irrespective of the party being internal or external (trunk call). The confirmation tone must also be heard by both the parties while **Call Unpark**.

Using Call Park from an attendant console

Procedure

1. Press the **start** button.
2. Dial the FAC for Call Park.
3. Dial the extension where the attendant wants to park the call.
4. Press the **release** button.

   An attendant can also use the Direct Extension Selection with Busy Lamp Field capability with the Call Park feature. For more information on the Direct Extension Selection with Busy Lamp feature, see *Administering Avaya Aura® Communication Manager*.

Parking a call using the trunk access code

Procedure

1. Press the **transfer** button.
2. Dial the trunk access code with the extension for parking a call.
3. Press the **transfer** button.

Retrieving a parked call

Procedure

To retrieve a call perform one of the following actions:

- Press the call park button that was used to park the call.
- Dial the FAC to retrieve parked calls.

  Note:

  If you need to retrieve the parked call from a different extension, dial the FAC followed by the extension the call is parked on.
- Press the unpark call button if administered on the SIP telephones.

Considerations for Call Park

This section provides information about how the Call Park feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Park under all conditions. The following considerations apply to Call Park:

- A User can park only one call at an extension at one time, even if the extension has multiple call appearances. A user can park a conference calls that has 2 to 5 participates. A user cannot park a conference call that has 6 participants. Similar behavior must be adhered when 12-party conference is enabled. A user cannot park a conference call that has 12 participants.
- Neither a user nor an attendant can park a call on a group extension. If a group member parks a call, the system parks the call at the extension of the group member. Group members can belong to the following groups:
  - A coverage answer group
  - A uniform call distribution (UCD) hunt group
  - A direct department calling (DDC) hunt group
  - A terminating extension group (TEG)
- If all appearances on a parked telephone are busy and no attendant or night-service extensions are configured when the call park timeout expires, the system:
  - Drops the call if a coverage path does not exist.
  - Does not drop the call if a coverage path exists.

Interactions for Call Park

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

Abbreviated Dialing

A user presses the **Abbreviated Dialing** button to park calls, or retrieve calls that are parked.

Attendant Console

Assign the common shared extensions to the optional Attendant Selector Console in the 00 through 09 block of numbers, on the bottom row, in any hundreds group so that the attendant can easily identify the extensions. The lamp that is associated with the number indicates “call parked” or “no call parked,” rather than a busy status or an idle status. For more information on the Attendant features, see *Administering Avaya Aura® Communication Manager*.

Automatic Wakeup

Neither a user nor an attendant can park Automatic Wakeup calls.

Bridged Call Appearance

If a user, that is active on a bridged call appearance, activates Call Park, the system parks the call on the primary extension associated with the bridged call appearance.

Call Vectoring

- Neither a user nor an attendant can park a call on a vector directory number (VDN) extension.
- Neither a user nor an attendant can park a call that is undergoing vector processing.

Code Calling Access

The system automatically parks a user or an attendant on the extension of the party that is paged when the user or attendant:

- Is using the Paging feature.
- Dials the Loudspeaker Paging Code Calling—TAC.
- Dials the extension of the party that is paged

Conference

Both users and attendants can park Conference calls.

Data Privacy and Data Restriction

The system automatically deactivates the Data Privacy feature and the Data Restriction feature when a user or attendant parks a call.

Drop

If a user receives an external call, and the user pushes the **drop** button after the user parks the call, the call is no longer parked.

If a user receives an internal call, and the user pushes the **drop** button after the user parks the call, the call remains parked. The system drops the call only when the user who parks the call hangs up.

Loudspeaker Paging Access

Neither a user nor an attendant can park calls to paging zones.

Remote Access

A Remote Access caller cannot park a call. However, the Code Calling Access feature, an answering attendant, or a telephone user can park an incoming Remote Access call.

Tenant Partitioning

If an attendant parks a call on a common shared extension, and tenant partitioning is inactive, the system routes the call to the attendant group when the call exceeds the call park timeout.

If an attendant parks a call on a shared extension, and tenant partitioning is active, the system routes the call to the attendant who parked the call when the call exceeds the park timeout interval.

The system functions as described in the preceding circumstances regardless of whether the **Deluxe Paging and Call Park Timeout to Originator** field of the Feature-Related System-Parameters screen is set to y or n.

Transfer

If the **Transfer Upon Hang-up** field on the Feature Related System-Parameters screen is set to y, a user does not need to press the **Transfer** button a second time to park a call.

Chapter 57: Call Pickup

Use the Call Pickup feature to answer calls for one another. The Call Pickup feature requires that users be members of the same pickup group.

- With the related Extended Call Pickup capability, users in one pickup group can answer the telephones for users in another pickup group.
- With the related Directed Call Pickup capability, users can specify what other telephone they want to answer. Pickup groups are not needed with Directed Call Pickup. You must first administer Directed Call Pickup before anyone can use this capability.

Detailed description of 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 may 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. However, if the system had selected the same extension the last time, then the system skips that extension and selects the next longest ringing extension.

Note:

Customized soft keys might not work when the Call Pickup feature is used.

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.

From Communication Manager Release 6.3.6 onwards , 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.

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.

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.

Enhanced Call Pickup Alerting

In Communication Manager Release 6.2 and later, Call Pickup Alerting provides the display of calling and called party information for all members of the pickup group and administrable alerting options. This feature works on DCP, H.323, and SIP stations.

When Enhanced Call Pickup is activated, the system updates the telephone displays of all members of the pickup group when another group member receives a call. The system provides the calling and called party information, which enables a member to decide whether to pick up the call or not. If a button is configured for call pickup, anytime you press the **call-pkup** button, the system shows the details of the incoming call.

The following alerting options are available:

Alerting option	Description
Tone options	• half-ring • intercom-ring
Ringer Types	• continuous: The system alerts the **call-pkup** button at five-second intervals. • if-busy-silent: If the station is busy on another call, the system does not alert the **call-pkup** button. • if-busy-single: If the station is busy on another call, the system alerts the **call-pkup** button only once. • no-ring: The system does not alert the **call-pkup** button. • single: The system alerts the **call-pkup** button only once. • triple: The system alerts the **call-pkup** button consecutively three times and then stops. This option is not available for SIP stations.

You can separately administer the time of the display and audible notifications. You must enable Call Pickup Alerting in your system.

Call Pickup administration

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

- Administering Call Pickup
  - Setting up Call Pickup
  - Enabling Call Pickup Alerting
  - Assigning a Call Pickup button to a user telephone
  - Assigning a Call Pickup Feature Access Code
- Maintaining Call Pickup
  - Removing a user from a pickup group
  - Deleting pickup groups
  - Changing a Call Pickup button on a user telephone
  - Removing a Call Pickup button from a user telephone
- Administering Extended Call Pickup
  - Setting up simple extended pickup groups
  - Setting up flexible extended pickup groups
  - Assigning a Call Pickup Extended button to a SIP telephone
- Maintaining Extended Call Pickup
  - Removing a pickup group from an extended pickup group
  - Changing extended pickup groups
- Administering Directed Call Pickup
  - Setting up Directed Call Pickup
- Maintaining Directed Call Pickup
  - Removing Directed Call Pickup from a user
- Administering Enhanced Call Pickup
  - Enabling Enhanced Call Pickup Alerting

Related links

Setting up Call Pickup on page 519
Enabling Call Pickup Alerting on page 520
Assigning a Call Pickup button to a user telephone on page 520

Assigning a Call Pickup feature access code on page 521
Removing a user from a call pickup group on page 521
Deleting pickup groups on page 521
Removing a Call Pickup button from a user telephone on page 522
Setting up simple extended pickup groups on page 523
Setting up flexible extended pickup groups on page 525
Assigning a Call Pickup Extended button to a SIP telephone on page 525
Removing a pickup group from an extended pickup group on page 522
Extended pickup group changes on page 527
Setting up Directed Call Pickup on page 527
Removing Directed Call Pickup from a user on page 530
Enabling Enhanced Call Pickup Alerting on page 520

Screens for administering Call Pickup

Screen Name	Purpose	Fields
Class of Restriction	Create a Class of Restriction (COR) for persons to use the Directed Call Pickup capability.	• Can Be Picked Up By Directed Call Pickup? • Can Use Directed Call Pickup?
	Create a Class of Restriction (COR) for audible indication of incoming calls to a member of the call pickup group.	Block Enhanced Call Pickup Alerting?
Extended Pickup Group	Combine pickup groups into an extended pickup group.	Pickup Group Number
Extended Pickup Groups	View how many extended pickup groups you have on your system.	All
Feature Access Code (FAC)	Assign pickup codes.	• Call Pickup Access Code • Directed Call Pickup Access Code • Extended Group Call Pickup Access Code
Feature-Related System Parameters	Enable the called pickup group member to join the call in progress that another group member has picked up.	Temporary Bridged Appearance on Call Pickup
	Enable Call Pickup Alerting	Call Pickup Alerting
	Enable the Directed Call Pickup capability.	Directed Call Pickup
	Enable the Extended Group Pickup capability.	Extended Group Call Pickup

Table continues…

Screen Name	Purpose	Fields
	Enable the Enhanced Call Pickup Alerting capability.	Enhanced Call Pickup Alerting
Pickup Group	Assign a user to a pickup group.	• Extended Group Number (only if you set your system for flexible extended pickup groups) • Group Name • Extension
Station	Assign a **Call Pickup button** button, **Directed Call Pickup** button, or a **Call Pickup Extended** button to a user extension. The **Call Pickup Extended** button is available only for a SIP station.	Button Assignments area
	Assign a COR to a user extension for Directed Call Pickup.	COR

Setting up Call Pickup

About this task

You can create one or many pickup groups, depending on your needs. A user extension can belong to only one pickup group.

Procedure

1. Add a pickup group and assign users to the pickup group.
2. Enable Call Pickup alerting.
3. Assign a **Call Pickup** button to each extension in the pickup group.
4. Assign a Feature Access Code (FAC).

Adding pickup groups

Procedure

1. Type `add pickup-group next`. Press `Enter`.

   The system displays the Pickup Group screen.

   The system also assigns the next available Group Number for the new pickup group.
2. Type a name for this pickup group in the **Group Name** field.
3. Type the extension of each group member.

   Up to 50 extensions can belong to one pickup group.
4. Press `Enter` to save your changes.

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

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. On page 19 of the Feature-Related System Parameters screen, set the **Call Pickup Alerting** field to `y`.
3. Select **Enter** to save your changes.

Enabling Enhanced Call Pickup Alerting

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. On page 19 of the Feature-Related System Parameters screen, set the **Enhanced Call Pickup Alerting** field to `y`.

   Note:

   The system displays the **Enhanced Call Pickup Delay Timer (sec.) Display** and **Audible Notification** fields only if the **Enhanced Call Pickup Alerting** field is set to y. To administer the alerting options for a button, set the button assignment by using the **`change station n`** command.
3. Type **`change cor n`**, where *n* is the COR number assigned to the station.
4. On page 2 of the Class of Restriction screen, set the **Block Enhanced Call Pickup Alerting** field to `n`.
5. Save the changes.

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.

Procedure

1. Get a list of all extended pickup groups.
2. Verify and delete the pickup group from all extended pickup groups.
3. 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**.

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.

Removing a pickup group from an extended pickup group

About this task

- 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 task.

Procedure

1. Type `change extended-pickup-group n`, where *n* is the extended pickup group that you want to check. Press `Enter`.
2. On the Extended Pickup Group screen, perform one of the following actions:
   - If the pickup group that you want to delete is not a member of this extended pickup group, press **Cancel**.
   - If the pickup group that you want to delete is a member of this extended pickup group:
     a. Select the pickup group.
     b. Press `Clear` or `Delete`, depending on your system.
     c. Press `Enter` to save your changes.
3. Repeat this procedure for each extended pickup group.

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.

Setting up simple extended pickup groups

About this task

What if you want to have members in one pickup group be able to answer calls for another pickup group? For 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.

Using extended pickup groups, the members of two or more individual pickup groups can answer each other's calls. In a simple extended pickup group, an individual pickup group can be assigned to only one extended pickup group.

All members of one pickup group can answer the calls to the other pickup groups within the simple extended pickup group.

Caution:

Before you administer what type of extended pickup group to use (none, simple, or flexible), be sure that your pickup group objectives are well thought out and defined.

Procedure

1. Set up the system for simple extended pickup groups.
2. Assign a FAC so that users can answer calls.

   Note:

   Instead of assigning a FAC, you can assign a **Call Pickup Extended** button for a SIP station.

3. Add pickup groups, if needed.

   If you need to create any pickup groups, see Setting up Call Pickup.

4. Assign pickup groups to an extended pickup group.

Related links

Setting up Call Pickup on page 519

Enabling simple extended pickup groups

Procedure

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

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

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.

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. Press `Enter`.

   The system displays the Extended Pickup Group screen.
2. In the **Pickup Group Number** column, type the numbers of the pickup groups that you want to link together.

   All members of each pickup group can answer calls to the other pickup groups in the extended group.
3. Press `Enter` to save your changes.

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.

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.

Assigning a Call Pickup Extended button to a SIP telephone

Procedure

1. Enter `change station n`, where *n* is the telephone number of the extension to which you want to assign a **Call Pickup Extended** button.
2. Click **Next** until you see the **Button Assignments** area.
3. Type `ext-pkup` next to the number of the button that you want the user to use to answer calls directly from another call pickup group.
4. Select **Enter** to save your changes.

Setting up flexible extended pickup groups

About this task

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.

Using Flexible extended pickup groups, members of one or more individual pickup groups can answer calls of another pickup group. However, the reverse scenario is not always true. With flexible extended pickup groups, you can prevent members of one or more pickup groups from answering the calls to another pickup group.

You can use Flexible extended pickup groups to control which 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.

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.

Procedure

1. Set up the system for flexible extended pickup groups.
2. Assign an FAC so that users can answer calls.

   To create an extended pickup group FAC, see Creating an extended pickup group Feature Access Code.

Note:

Instead of assigning a FAC, you can assign a **Call Pickup Extended** button for a SIP station.

3. Add or change pickup groups, and point a pickup group to an extended pickup group.

Creating flexible extended pickup groups

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. On the Feature-Related System Parameters screen, click **Next** until you see the **Extended Group Call Pickup** field.
3. In the **Extended Group Call Pickup** field, type `flexible`.
4. Press `Enter` to save your changes.

Associating individual pickup groups with an extended pickup group

Procedure

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

   If you set the **Extended Group Call Pickup** field on the Feature-Related System Parameters screen to flexible, the system displays the **Extended Group Number** field on the Pickup Group screen.

   Important:

   If you change your system from simple to flexible extended pickup groups, see Extended pickup groups, the system automatically populates the **Extended Group Number** field on the Pickup Group screen for each pickup group member. For example, if pickup groups 13 and 14 are members of extended pickup group 4 and you change the system from simple to flexible extended pickup groups, the system automatically populates the **Extended Group Number** field to 4 on the Pickup Group screen for these two pickup groups. You are not required to keep the number that the system automatically populates in the **Extended Group Number** field. You can change the number in the **Extended Group Number** field to another pickup group number. You can also make the field blank.

2. If you want to associate, or point, the pickup group to an extended pickup group, type the number of the extended pickup group for which this pickup group can answer calls in the **Extended Group Number** field.

   This pickup group answers calls for any pickup group that is a member of the extended pickup group you enter.

3. Press `Enter` to save your changes.

Related links

Extended pickup group changes on page 527

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. Press `Enter`.

   The system displays the Extended Pickup Group screen.

2. In the **Pickup Group Number** column, type the number of the pickup group that you want add to this extended pickup group.
3. Press `Enter` to save your changes.

Extended pickup group changes

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.

From simple to flexible

If you want to change all extended pickup groups from simple to flexible, you can easily make the change. See Creating flexible extended pickup groups on page 526. 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.

From flexible to simple

The process is more complex to change all extended pickup groups from flexible to simple. Before you can change the extended pickup group from flexible to simple, you must first delete all of the individual pickup groups from all of the extended pickup groups. Then you can change the extended pickup group from flexible to simple (see Enabling simple extended pickup groups on page 523). After that step, you must re-administer all of the extended pickup groups again.

Related links

Creating flexible extended pickup groups on page 526
Enabling simple extended pickup groups on page 523

Setting up Directed Call Pickup

About this task

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) supporting this feature.
- Telephones that can answer another extension using Directed Call Pickup must have a COR supporting this feature.

Procedure

1. Determine if Directed Call Pickup is enabled on your system.

2. Create one or more Classes of Restriction (COR) for Directed Call Pickup.
3. Assign the COR to individual extensions.
4. Assign a **Directed Call Pickup** button to each extension that is assigned the COR.
5. Assign a Feature Access Code (FAC).

Enabling Directed Call Pickup

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`. Press `Enter`.

   The system displays the Feature-Related System Parameters screen.
2. Click **Next** until you see the **Directed Call Pickup?** field.
3. Set the **Directed Call Pickup?** field to `y`. Press `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.

End-user procedures for Call Pickup

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Related links

Using Directed Call Pickup to answer a call on page 531
Using Call Pickup to answer a call on page 531

Using the Extended Group Pickup FAC on page 531
Using the Call Pickup Extended button on a SIP station on page 531

Using Call Pickup to answer a call

Procedure

1. Disconnect the call.
2. Perform one of the following actions:
   - Press the **call-pkup** Call Pickup button.
   - Dial the Call Pickup FAC.

Using Extended Group Pickup to answer a call

Using the Extended Group Pickup FAC

Procedure

1. Disconnect the call.
2. Dial the Extended Group Pickup FAC.
3. Dial the unique Pickup Number of the pickup group in the extended pickup group.

   Each pickup group within an extended pickup group has a unique Pickup Number.

Using the Call Pickup Extended button on a SIP station

Procedure

1. Press the **Call Pickup Extended** button.
2. Dial the unique Pickup Number of the pickup group in the extended pickup group.

Using Directed Call Pickup to answer a call

Procedure

1. Disconnect the call.
2. Perform one of the following actions:
   - Press the **dir-pkup** for Directed Call Pickup button.
   - Dial the Directed Call Pickup FAC.
3. Wait for dial tone.
4. Dial the extension that you want to pick up.

Considerations for Call Pickup

This section provides information about how the Call Pickup feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Pickup under all conditions.

- Exclusion is not supported for call pickup calls.
- A member of a pickup group who makes a call to another group member cannot use Call Pickup to answer the call.
- The called party cannot answer the call using Call-Pickup display, this will drop the call. Called party should answer the call using primary call-appearance.
- You can use the Team Button feature for call pick up. For more information, see the feature description on Team Button.

Interactions for Call Pickup

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

Abbreviated Dialing

A user can use a single **Abbreviated Dial** button to store either:

- Both the Feature Access Code (FAC) for Directed Call Pickup and a telephone number
- Only the FAC for Directed Call Pickup

Attendant

An attendant can use the Directed Call Pickup capability to answer calls. However, other users cannot use the Directed Call Pickup capability to answer a call that alerts at an attendant console.

Automatic Callback and Ringback Queuing

Neither the call pickup group members nor the Directed Call Pickup users can answer ringout calls. For information on ringout calls, see Detailed description of Automatic Callback on page 277.

Bridged Call Appearance

Calls that are made to a primary telephone, alerting at bridged appearances of the primary telephone, can only be answered by pickup group members of the primary number.

- If the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to n, the primary appearance and all bridged appearances of the call are dropped after Call Pickup is used to answer the call.
- If the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to y, the primary and bridged call appearance lamps stay lit after Call Pickup is used to answer the call.

- If the primary telephone and the bridged telephone are both in the same pickup group, members in the pickup group can answer a call that is made to the primary telephone that is ringing at the bridging user's telephone. This can be done instead of selecting the bridged appearance button.
- If the primary telephone and the bridged call appearance are not in the same pickup group, members who are in the same pickup group as the bridged call appearance telephone cannot answer a call that is made to the primary telephone.
- If Call Pickup Alerting is active, and a bridged call appearance rings on the telephone of a member of a call pickup group that is also getting a direct call, other group members cannot answer the direct call.
- If Call Pickup Alerting is inactive, and a bridged call appearance rings at the telephone of a member of a call pickup group that is also getting a direct call, other group members can answer the direct call.
- You cannot use the Directed Call Pickup capability to answer a call that alerts at a bridged call appearance. You can use Directed Call Pickup to answer the call using the primary extension.

Call Coverage

If a user has a call-coverage temporary bridged appearance, the user can use Directed Call Pickup to answer a redirected call that alerts at the telephone of another covering user.

Call Detail Recording (CDR)

CDR records the extension number that the caller dials.

Call Forwarding

If the Temporary Bridged Appearance capability on the Call Pickup feature is enabled, the system maintains a temporary bridged appearance if the forwarded-to extension belongs to the same call pickup group as the forwarded-from extension. If the Temporary Bridged Appearance capability on the Call Pickup feature is disabled, the system does not maintain a temporary bridged appearance.

Call Pickup Alerting

When a pickup group member uses the Directed Call Pickup capability to answer a ringing call of another group member, and the call is the only call that is ringing for any member of the pickup group, the call pickup alerting lamp goes out.

Call Waiting

A user cannot use the Call Pickup capability to answer a Call Waiting call.

Class of Restriction (COR)

The Call Pickup and Directed Call Pickup features override any restrictions that are set by the **Calling Permissions** fields on the Class of Restriction screen.

Conference

If call pickup alerting is enabled, and a user uses the Conference feature after the user answers the call, the call pickup status lamp goes out. If additional calls come into the pickup group, the status lamp of the user flashes.

Consult

If the Temporary Bridged Appearance capability is disabled for the Call Pickup feature, the system presents a Consult call from the covering user as an idle call appearance.

Expert Agent Selection (EAS)

EAS agents use the Directed Call Pickup capability to:

- Have other agents answer their calls
- Answer the calls of other agents

The Class of Restriction (COR) of the agent overrides the COR of the extension where the agent is logged in.

If an agent is logged in to a telephone extension, and if the Directed Call Pickup capability is active for both the agent and the extension, the user can use either the agent Login ID or the telephone extension to answer the call with Directed Call Pickup.

Chapter 58: Call Waiting Termination

Use the Call Waiting Termination feature to automatically notify a user with a single-line telephone who is active on a call, that a second call is waiting.

Detailed description of Call Waiting Termination

Users with a single-line telephone can place a call on hold to answer a waiting call. After a user answers the call that is waiting, the user can return to the call that is held, or the user can toggle back and forth between the two calls. A user with a single-line telephone can connect to only one call at a time.

Call Waiting tones

When a call is waiting for a user, the user hears:

- One quick burst of tone when a call from another user is waiting
- Two quick bursts of tone when an outside call, or a call that is handled by an attendant, is waiting
- Three quick bursts of tone when a priority call is waiting

Note that the system does not support special ring tones over direct inward dialing (DID) facilities.

A priority call can wait for the telephone to become idle even if Call Waiting Termination is deactivated. However, if an attendant handles the call, the user hears a busy tone, unless the **Attendant Call Waiting Indication** field on the Station screen is set to y.

You assign Call Waiting Termination on a per-telephone basis. For a virtual extension, you assign Call Waiting Termination on the physical telephone.

Call Waiting Termination administration

The following tasks are part of the Call Waiting Termination feature:

- Administering Call Waiting Termination system parameters
- Assigning Call Waiting Termination

Related links

Administering Call Waiting Termination system parameters on page 536
Assigning Call Waiting Termination on page 536

Screens for administering Call Waiting Termination

Screen name	Purpose	Fields
Feature-Related System Parameters	Specify that a user or an attendant hears a repetitive tone when a call is waiting.	Repetitive Call Waiting Tone?
	Specify the number of seconds between each repetitive call waiting tone.	Repetitive Call Waiting Interval (sec)
Station	Enable the Call Waiting Termination feature for a user.	Call Waiting Indication
	Enable the Call Waiting Termination feature for an attendant.	Att. Call Waiting Indication

Administering Call Waiting Termination system parameters

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. On the Feature-Related System Parameters screen, click **Next** until you see the **Repetitive Call Waiting Tone** field.
3. In the **Repetitive Call Waiting Tone** field, perform one of the following actions:
   - If you want the users and the attendants to hear a repetitive call waiting tone when the users and attendants use the Call Waiting Termination feature, type `y`.
   - If you do not want the users and the attendants to hear a repetitive call waiting tone when the users and the attendants use the Call Waiting Termination feature, type `n`..
4. In the **Repetitive Call Waiting Interval (sec)** field, type the number of seconds between the repetitive call waiting tones.
5. Press `Enter` to save your changes.

Assigning Call Waiting Termination

Procedure

1. Type `change station` *n*, where *n* is the extension to which you want to assign the Call Waiting Termination feature. Press `Enter`.
2. On the Station screen, click **Next** until you see the **Call Waiting Indication** field.

3. In the **Call Waiting Indication** field, perform one of the following actions:
   - If you want to activate Call Waiting Termination for the user, type `y`.

     If you set the **Call Waiting Indication** field to y, calls that a user or an attendant originate, and calls that originate from the outside, wait at the single-line telephone if the telephone is busy. The system sends a distinctive call-waiting tone to the user.

     The system denies the Call Waiting Termination feature to a user if any of the following conditions are true:

     - **Data Restriction** field on the Station screen is set to y.
     - **Switchhook Flash** field on the Station screen is set to n.
     - Class of Service that you assign to the user activates the Data Privacy feature for the user.
   - If you want to deactivate Call Waiting Termination for the user, type `n`.
4. In the **Att. Call Waiting Indication** field, perform one of the following actions:
   - Type `y` to activate Attendant Call Waiting Termination for the user.

     If you set the **Att. Call Waiting Indication** field to `y`, calls that an attendant originates, or that an attendant extends, wait at the single-line telephone if the telephone is busy. The system sends a distinctive call-waiting tone to the user.

     The system denies the Call Waiting Termination feature to a user if any of the following conditions are true:

     - **Data Restriction** field on the Station screen is set to y.
     - **Switchhook Flash** field on the Station screen is set to n.
     - Class of Service (COS) that you assign to the user activates the Data Privacy feature for the user.
   - Type `n` to deactivate Call Waiting Termination for the user.
5. Press `Enter` to save your changes.

Considerations for Call Waiting Termination

This section provides information about how the Call Waiting Termination feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Waiting Termination under all conditions. The following considerations apply to Call Waiting Termination:

- Call Waiting is available only for users who have single-line telephones. Calls to multiple-appearance telephones do not wait, because the system routes these calls to an idle call appearance.

- An analog telephone user must place the active call on soft hold, and dial the Answer Hold-Unhold Feature Access Code, to answer the waiting call.
- If you activate Call Waiting for a user of an analog single-line telephone, and the user starts a conference call, the system denies the Call Waiting feature to the user while the user is on the conference call.

Interactions for Call Waiting Termination

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

- The system denies the use of the Call Waiting Termination feature when any of the following conditions or features are active at a single-line telephone:
  - Another Call Waiting call
  - Automatic Callback (to or from the telephone)
  - Data Privacy
  - Data Restriction
- Call Pickup and Directed Call Pickup

  A member of a call pickup group cannot use the Call Pickup feature or the Directed Call Pickup capability to pick up a Call Waiting call.

Chapter 59: Call-by-Call Service Selection

Using the Call-by-Call (CBC) Service Selection feature, a single ISDN trunk group can carry calls to several services. Call-by-Call Service Selection eliminates the need to dedicate each trunk group to a specific service. With Call-by-Call Service Selection, you can set up various voice and data services and features for a particular call.

Call-by-Call Service Selection provides the following benefits:

- Cost reduction. Since many services share the same trunks, this feature can reduce the total number of trunks that you must use.
- Improved service. Features and services are less likely to be blocked.
- Simplified networking. This feature simplifies network engineering. Instead of a per-service basis, you can analyze trunking needs based on total traffic.
- Tracking. Call-by-Call Service Selection calls are measurable.

Detailed description of Call-by-Call Service Selection

Call-by-Call Service Selection uses the same route patterns and route preferences as Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), and Generalized Route Selection (GRS). The system uses information that is assigned in the AAR, ARS, GRS route patterns to determine what service or facility to use on an outgoing Call-by-Call Service Selection call.

You can administer a variety of services to use a single trunk group. The system distributes traffic over all available trunks for increased efficiency. Then you can assign services that are used on incoming and outgoing Call-by-Call Service Selection calls.

Using Country Protocol 1, you can integrate services such as MEGACOM, ACCUNET, and INWATS onto a single ISDN trunk group, with flexible assignment of trunks to each service. Calls such as an incoming 800 service call that requires through-switching as an outgoing WATS call can be routed over the same facility.

Call-by-Call Service Selection example

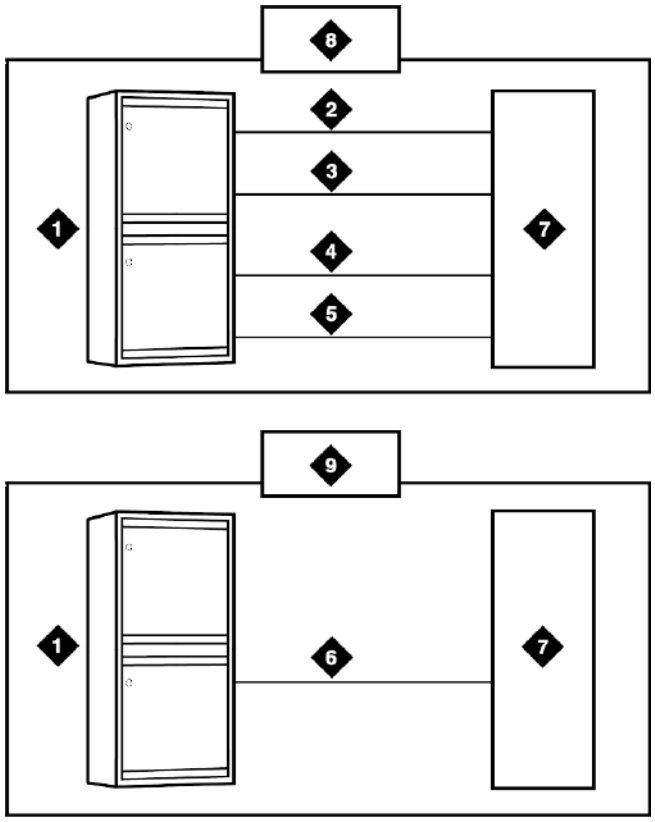


Figure 9: Call-by-Call Service Selection example

Table 70: Figure notes:

1. Avaya S8XXX Server
2. MEGACOM trunk group
3. MEGACOM 800 trunk group
4. Software-defined network (SDN) trunk group

1. OUTWATS trunk group
2. Call-by-Call Service Selection trunk group
3. Public switched network
4. Without Call-by-Call Service Selection
5. With Call-by-Call Service Selection

ISDN messages and information elements for usage allocation

Using Call-by-Call Service Selection, the system can specify service types on a call-by-call basis. To specify service types, you assign incoming calls to an ISDN Call-By-Call trunk group based on the number of the called party.

You can also specify service types in a SETUP message. This message indicates that the originating system intends to use the specified service or facility to initiate a call. The SETUP message can contain units called Information Elements (IE) that specify call-related information. Call-by-Call Service Selection uses the following IEs:

Network-Specific Facility (NSF)

Network-Specific Facility (NSF) indicates which facilities or services are used to complete the call. NSF is usually not used outside the US and Canada.

The system also checks all incoming ISDN trunk calls for the presence of an NSF IE. If an NSF IE is present, the system ensures that the requested service is compatible with the trunk administration before the system accepts the call.

For an outgoing CBC trunk group, the system uses the service or the feature that is specified on the selected route pattern for the call to construct the NSF IE.

If an associated NSF does not exist for the specified service or feature, the system does not send an NSF IE. For example, SETUP messages for incoming and outgoing calls that are classified only by a called-party number do not contain an NSF IE.

Transit Network Selection

Transit Network Selection indicates which interexchange carrier (IXC) the system uses on an inter-LATA call.

If a call requires both the service or the feature and the IXC to be specified, the system sends the IXC information in the NSF IE, instead of in the Transit Network Selection IE.

Usage Allocation Plans for Call-by-Call Service Selection

You can assign Usage Allocation Plans (UAPs) to provide more control over a Call-by-Call Service Selection trunk group. You can allocate a minimum and a maximum number of channels for incoming and outgoing called numbers, privileged users, and voice and data calls.

With a UAP, you can set the:

- Maximum number of trunks that each service can use at any given time. The sum for all services can exceed the total number of trunk group members. For example, for a 15-member trunk group, you can administer a maximum of seven MEGACOM service calls, six MEGACOM 800 service calls, and eight software-defined network (SDN) calls. Using UAP, you can ensure that a specific service does not dominate all trunk group members, yet is flexible to accommodate fluctuating demands.
- Minimum number of trunks that must always be available for each service. The sum for all services cannot exceed the total number of trunk group members. For example, for a 10-member trunk group that provides access to MEGACOM service, MEGACOM 800 service, and SDN service, the minimum number of trunks to use for each of these services cannot add up to more than 10.

When these UAP limits are exceeded, the system rejects the call, even if a trunk is available. On outgoing calls, the calling party hears a reorder tone, unless other routing preferences are available.

You can assign either a fixed or a scheduled UAP for each Call-by-Call Service Selection trunk group.

- With a fixed UAP, one plan applies at all times.

- With a scheduled UAP, you can administer different plans to apply at different times of the day and on different days of the week. You can assign as many as six activation times and associated plans for each day of the week.

You can administer a simple fixed UAP, or a flexible UAP with many scheduling options. You can even start out with no UAP, and then build the UAP as needed.

Call-by-Call Service Selection incoming call-handling treatment

Call-by-Call Service Selection provides special incoming call-handling treatment for ISDN and SIP trunk groups. The system handles an incoming call on an ISDN or SIP trunk according to a treatment table that you administer for the trunk group. Depending on the platform that you use, a different number of combinations of call treatments are possible in the treatment table.

The system selects the treatment for an incoming call based on the first three columns of the Incoming Call-Handling Treatment (ICHT) screen. When the attributes of an incoming call match these specifications, the system treats the call according to the corresponding entries in the next four columns of the table. If an incoming call matches more than one set of specifications, the most restrictive case applies. The following table lists the possible cases from most restrictive to least restrictive.

	Service or feature	**Called len**	**Called number**
Most restrictive	Specified	Specified	*x* leading digits specified
	Specified	Specified	*y* leading digits specified, where *y* < *x*
	Specified	Specified	Not specified
	Specified	Not specified	Not specified
	Other	Specified	*x* leading digits specified
	Other	Specified	*y* leading digits specified, where *y* < *x*
	Other	Specified	Not specified
Least restrictive	Other	Not specified	Not specified

Call Detail Recording with Call-by-Call Service Selection

On successful call attempts that use ISDN CBC trunk groups, Call Detail Recording (CDR) records the NSF that the NSF IEs of the call specify. CDR refers to this information as the ISDN Network Service (INS). The value that is passed to CDR is the 3-digit equivalent of the NSF IE. The system also records NSF information for Facility Type 2 calls that use ISDN Call-by-Call trunk groups, if the NSF is available in the incoming SETUP message.

If an outgoing Call-by-Call Service Selection call uses an interexchange carrier other than the presubscribed common carrier, CDR records the 3-digit or the 4-digit Interexchange Carrier (IXC) Code . CDR might not record the IXC properly if the dialed-code format differs from the US IXC code formats.

When a Call-by-Call Service Selection call is rejected because of a UAP, CDR records the cause as an ineffective call attempt. The NSF recording also occurs for the user-defined Facility Type 2. However, the NSF recording occurs only if the NSF is available in the incoming SETUP message.

Call-by-Call Service Selection administration

You administer Call-by-Call Service Selection on a per-trunk-group basis.

The following steps are part of the administration process for the Call-by-Call Service Selection feature:

- Setting up a trunk group for CBC
- Administering incoming call handling treatment
- Administering route patterns for the CBC trunk group
- Administering network facilities

Related links

Setting up a trunk group for CBC on page 544
Administering incoming call handling treatment on page 545
Administering route patterns for the CBC trunk group on page 545
Administering network facilities on page 546

Preparing to administer Call-by-Call Service Selection

Procedure

1. Type `display system-parameters customer-options`. Press `Enter`.

   The system displays Optional Features screen.

2. Ensure that the following fields are set to y:

   - **ISDN**
   - **ISDN-BRI Trunks**
   - **Usage Allocation Enhancements**

   If any of these fields is set to n, your system might not support the Call-by-Call Service Selection feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Call-by-Call Service Selection, or to open a service request.

Screens for administering Call-by-Call Service Selection

Screen name	Purpose	Fields
Optional Features	Ensure that the proper license fields are set to y.	• ISDN-PRI • ISDN-BRI Trunks • Usage Allocation Enhancements
ISDN Trunk Group	Indicate the service for which this trunk group is dedicated.	• Service Type • Usage Alloc • All fields on the CBC Trunk Group Usage Allocation screen • All fields on the CBC Trunk Group Usage Allocation Plan Assignment Schedule screen
Incoming Call Handling Treatment	Specify call handling for ISDN and SIP trunk groups.	• All fields on the Incoming Call Handling Treatment (ICHT) Table screen
Route Pattern	Administer the route patterns to use with this trunk group.	• IXC • Service/Feature • Band
Network-Facilities	Administer network facilities for Call-by-call Service Selection.	All

Setting up a trunk group for CBC

Procedure

1. Type `change trunk-group n`, where *n* is the ISDN trunk group that you want to designate for Call-by-Call Service Selection.

   If you want to add a new trunk group, type `add trunk-group x`, where *x* is the next unused trunk group number.

   The system displays the ISDN Trunk Group screen.

2. In the **Group Type** field, type `isdn`.

   The system displays additional ISDN-specific fields.

3. In the **Service Type** field, type `cbc` for Call-by-call Service Selection.

4. In the **Usage Alloc?** field, type `y` to allocate the service that the trunk group provides.

5. Click **Next** until you see the CBC Trunk Group Usage Allocation page.

6. In the **Service/Feature** field under the **Usage Allocation Plan 1** column, type the name of the service for which you want to allocate CBC trunk service.

   You can administer up to three (UAPs) for each trunk.

7. In the **Min # Chan** and **Max # Chan** fields, type a minimum number and a maximum number of channels for incoming and outgoing called numbers, privileged users, and voice and data calls.
8. Repeat steps 8 and 9 for each service for which you want to allocate CBC trunk service.
9. Click **Next** until you see the CBC Trunk Group Usage Allocation Plan Assignment Schedule page.
10. In the **Fixed** field, perform one of the following actions:
    - Type `y` if you want a specific UAP to be activated at all times for this trunk group. If you type `y`, the system displays **Allocation Plan Number** field.
    - Type `n` if you do not want a fixed UAP to be activated at all times for this trunk group.
11. In the **Allocation Plan Number** field, type the number of the UAP that you want to be activated at all times for this trunk group.
12. In the **Scheduled** field, type `y` if you want to administer a schedule that can change up to six times a day for each day of the week.
13. For each day of the week, use the **Act Time** and the **Plan #** fields to type the activation time, and the type of UAP to use at different times of the day.
14. Press `Enter` to save your changes.

Administering incoming call handling treatment

Procedure

1. Type `change inc-call-handling-trmt`.
2. On the Incoming Call Handling Treatment screen, complete the fields for each Call-by-Call Service Selection service.

Note:

For SIP trunk groups, the **Per Call CPN/BN** and **Night Serv** fields do not appear on the Incoming Call Handling Treatment screen. For more information on the Incoming Call Handling Treatment screen, see *Avaya Aura® Communication Manager Screen Reference*.

Administering route patterns for the CBC trunk group

Procedure

1. Type `change route-pattern n`, where *n* is the number of the route pattern that you want to administer.

   The system displays the Route Pattern screen.
2. In the **IXC** (Interexchange Carrier) field, identify the carrier, such as AT&T, that the system uses for calls that are routed over an IXC, and for Call Detail Recording (CDR).

   This field can also be left blank.

3. In the **Service/Feature** fields, type the name of the service that is associated with this route pattern.
4. If the value in the **Service/Feature** field is outwats-bnd, use the **Band** field to enter a number that represents the OUTWATS band number (US only).
5. Press `Enter` to save your changes.

Note:

For more information on the Route Pattern screen, see *Avaya Aura® Communication Manager Screen Reference*.

Administering network facilities

About this task

The Network Facilities screen supports the Call-by-Call Service Selection feature for ISDN trunks. Only Avaya personnel can administer these predefined services and features. If the **Usage Allocation Enhancement** field on the Optional Features screen is set to y, you can administer the **Additional Services/Features** fields.

Procedure

1. Type `change isdn network-facilities`. Press `Enter`.

   The system displays the Network Facilities screen.
2. In the **Name** field, type up to 15 alphanumeric characters to specify the name of the indicated service or feature.
3. In the **Facility Type** field, perform one of the following actions:
   - If the associated entry is a feature, type `0`.
   - If the associated entry is a service, type `1`.
   - If the associated entry is of type incoming, type `2`.
   - If the associated entry is of type outgoing, type `3`.

   Note:

   You can administer types 2 and 3 if the **Usage Allocation Enhancements** field on the Optional Features screen is set to y.

   If the **Facility Type** field is set to either 0 or 1, the **Facility Coding** field displays five binary values. These values specify the ISDN encoding value of the associated service or feature.
4. Press `Enter` to save your changes.

Interactions for Call-by-Call Service Selection

This section provides information about how the Call-by-Call Service Selection feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Call-by-Call Service Selection in any feature configuration.

Call Detail Recording (CDR)

On successful call attempts that use ISDN Call-By-Call trunk groups, CDR records the Network-Specific Facility (NSF) that is specified by the NSF IE of the call. CDR refers to this information as the ISDN Network Service (INS). The value that is passed to CDR is the 3-digit equivalent of the NSF IE. NSF information for Facility Type 2 calls, which is used with ISDN Call-by-Call trunk groups, is also recorded if the NSF is available in the incoming SETUP message.

If an outgoing Call-by-Call Service Selection call uses an interexchange carrier (IXC) other than the presubscribed common carrier, CDR records the 3-digit or the 4-digit IXC code . CDR might not record the IXC code properly if the dialed-code format differs from the IXC formats that are used in the US.

When a Call-by-Call Service Selection call is rejected because of a Usage Allocation Plan (UAP), CDR records the cause as an ineffective call attempt. The NSF recording also occurs for the user-defined Facility Type 2 call. However, the NSF recording occurs only if the NSF is available in the incoming SETUP message.

Generalized Route Selection (GRS)

Call-by-Call Service Selection uses the same routing tables and routing preferences that GRS uses.

Multiquest Flexible Billing

Do not use a service or a facility with the Facility Type set to 2 or 3. NSF processing is not performed for Facility Type 2. An NSF is excluded from the outgoing SETUP message for Facility Type 3.

Time-of-Day Routing

Any Time-of-Day Routing administration that affects routing preference also affects Call-by-Call Service Selection. Use Time-of-Day Routing to vary the IXC, based on the time of day and the day of week.

Traffic Measurements

The system provides traffic measurements for each service that is administered for an ISDN Call-by-Call Service Selection trunk group.

Chapter 60: Caller ID

Use the Caller ID feature to interpret calling party information that is signaled over ISDN or H.323 trunks, and displaying the calling party number on your display telephone. Caller ID is also known as Incoming Call Line Identification (ICLID).

Detailed description of Caller ID

The Caller ID feature displays calling party information on your display telephone that is signaled over ISDN or H.323 trunks.

- For a description about calling party information that is signaled over multifrequency (MF) or Session Initiation Protocol (SIP) trunks to your display telephone, see the Automatic Number Identification feature.
- For a description about calling party information that is signaled over Centralized Automatic Message Accounting (CAMA) trunks to your local emergency rapid response organization, see the E911 feature.

Communication Manager stores and displays up to 15 characters of caller ID information, which the central office (CO) sends on incoming calls. If the information is longer than 15 characters, the software truncates the information to 15 characters. If the caller ID information is not received, the system displays the trunk group name and the trunk access code (TAC).

In the US, the CO sends both calling party name and calling party number, if this information is available. In Japan, the CO sends only the calling party number. This information is sent on a CO loop-start trunk in the US. In Japan, this information is sent on either a CO loop-start trunk, a Direct Inward Dialing (DID) trunk, or a Direct Inward and Outward Dialing (DIOD) trunk.

Caller ID on analog trunks

Caller ID on analog trunks is also known as Bellcore Calling Name ID. The system uses this capability to accept calling name information from a local exchange carrier (LEC) network that supports the Bellcore calling name specification. The system can also send calling name information in the correct format if Bellcore calling name ID is properly administered. The following caller ID protocols are supported:

- Bellcore (default). US protocol (Bellcore transmission protocol with 212 modem protocol)
- V23-Bell. Bahrain protocol (Bellcore transmission protocol with V.23 modem protocol)

Caller ID on digital trunks

In the US, a CO can send the calling party name and the calling party number over digital trunks for display on digital telephones. The display of the calling party name and the calling party number works with all Communication Manager Digital Communications Protocol (DCP) and Basic Rate Interface (BRI) digital telephones that have either a 40-character or a 32-character alphanumeric display.

Caller ID administration

The following step is part of the administration process for the Caller ID feature:

- Displaying Caller ID information

Related links

Displaying Caller ID information on page 550

Preparing to administer Caller ID

Procedure

1. Type `display system-parameters customer-options`. Press `Enter`.
2. Ensure that the **G3 Version** field is set to V6 or later.
3. Ensure that the **Analog Trunk Incoming Call ID** field is set to y.

   Note:

   If the **G3 Version** field is not set to V6 or later, or if the **Analog Trunk Incoming Call ID** field is set to n, your software does not support the Caller ID feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering a caller ID, or to open a service request.
4. Exit the screen.

Screens for administering Caller ID

Screen name	Purpose	Fields
Optional Features	Ensure that the **Analog Trunk Incoming Call ID** field is set to y.	Analog Trunk Incoming Call ID
Trunk Group	Set this field to 120 for Caller ID.	Incoming seizure (msec)
	Set up the trunk group to receive caller ID information.	Receive Analog Incoming Call ID
	Set to incoming or two-way.	Direction

Displaying Caller ID information

Procedure

1. Type `change trunk group n`, where *n* is the number of the trunk group for which you want to set up Caller ID.

   If you want to set up a new trunk group, type `add trunk group next`.

   The system displays the Trunk Group screen.
2. In the **Group Type** field, type `co`, `did`, or `diod`.
3. In the **Direction** field, type `incoming` or `two-way`.

   Note:

   When the **Group Type** is diod, the **Direction** field defaults to two-way. When the **Group Type** is did, the **Direction** field is hidden, because all calls are incoming.
4. Click **Next** until you see the **Trunk Features** section.
5. In the **Receive Analog Incoming Call ID** field, type `Bellcore` for the US, or `NTT` for Japan.
6. Click **Next** until you see the **Administrable Timers** section.
7. In the **Incoming Seizure (msec)** field, type `120`.
8. Press `Enter` to save your changes.

Considerations for Caller ID

This section provides information about how the Caller ID feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Caller ID under all conditions. The following consideration apply to Caller ID:

- If you use Incoming Caller ID on analog trunks that are connected to a Direct Inward and Outward Dialing (DIOD) central office (CO) trunk media module, do not put these trunks in an outgoing Automatic Alternate Routing (AAR) or an Automatic Route Selection (ARS) route pattern. The loop-start trunks that the DIOD CO trunk media module supports do not provide answer supervision. Thus, the potential for toll fraud exists.

Interactions for Caller ID

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

Attendant Display Features

A call that is redirected to either the attendant or the attendant queue causes the display on the station of the attendant to match that of the station display of the connected party.

Automatic Display of Incoming Call Identification

If a new call comes in while the station user is off-hook and connected to a call, the display automatically shows the new incoming call identity for 30 seconds. After 30 seconds, the display returns to the identity of the original call. If the system redirects the call after a few rings, the display returns to the identity of the original call. If the system shows a new incoming call, and then that call drops, the display returns to the identity of the original call.

Bridged Call

The system shows incoming call identity on both the primary station and the bridged station.

Call Forwarding

Forwarded-From Station Display:

The system does not show any information on the station of the called principal.

Forwarded-To Station Display:

The system shows the identity of the calling party and the called party, and the reason (R) code. If the forwarded-to station is on a different switch, the system does not forward the called party information.

Call Pickup

Called Party Station Display:

Shows the identity of the calling party.

Answering Party Station Display:

If Call Pick-Up answers a Caller ID call, the system shows the identities of both the calling party and the called party.

Call Coverage

Called Party Display:

The display of the called party shows the identity of the calling party until the coverage party answers the call. If the coverage party answers the call, the station display of the called party goes blank. If the called party temporarily bridges in after the coverage party answers the call, the displays of the coverage party and the called party change to indicate a conference call.

Coverage User Station Display:

The station display of the coverage user shows the same display as the station display of the connected party.

Call Vector Routing

When a Caller ID call coming from analog trunks transfers to a Vector Directory Number (VDN), the incoming calling number is directed to that VDN so call vector routing can be based on the caller ID information.

The Automatic Number Identification (ANI) that is received for the incoming call, by way of inband signaling or ISDN, is forwarded with a route-to step over a trunk that supports inband or ISDN ANI delivery.

Distributed Communications System (DCS)

If Communication Manager has both DCS and Integrated Services Digital Network (ISDN) displays, the system shows the caller ID information in DCS formats.

Hold

When Hold is activated, the display becomes blank. The party who activates the Hold then reads the identity of the newly connected party. The display of the held station remains unchanged. When the party deactivates the Hold, the system refreshes the display to indicate the current state of the call.

Malicious Call Trace (MCT)

When MCT is activated for a particular call, the system displays incoming calling numbers to controller stations.

Tandem Operations

The system passes the calling party name and the calling party number to the terminating server over ISDN trunks with DCS Plus (+).

Transfer

When the system transfers an Caller ID call, the display of the transferred-from station becomes blank. The display of the transferred-to station shows the identity of the transferred-from party if the transfer is not yet complete. Once the transfer is complete, the transferred-to station shows the identity of the calling party.

Chapter 61: Centralized Attendant Service

Using the Centralized Attendant Service (CAS) feature, attendants within a private network can serve all branch locations from a central or a main location. Each branch in a centralized attendant service has its own listed directory number (LDN) or other type of access from the public network. With this feature, the system routes incoming calls to a branch, and calls that users make directly to the attendants, to the centralized attendant. CAS uses release link trunks (RLT) to direct calls.

Detailed description of Centralized Attendant Service

With Centralized Attendant Service (CAS), you can provide attendant services in a private network from a central location.

The CAS main system operates independently of the individual CAS branch systems. The operation for CAS main system traffic is identical to the operation of a stand-alone system.

Each branch in a CAS network connects to the main office through RLTs. These trunks provide paths to:

- Send incoming attendant-seeking trunk calls at the branch to the main location for processing and extend the calls back to the branch. Both parts of a call use the same trunk.
- Return timed-out waiting and held calls from the branch to the main location.
- Route calls from the branch to the main location.

Two queues are associated with CAS calls. One queue is at the main office, and the other queue is at the branch. If idle RLTs are available from the branch to the main location, RLTs are seized. CAS calls are then queued at the main location, along with other attendant-seeking calls. If all RLTs are in use, CAS calls to the attendant are queued at the branch in an RLT queue. The length of the queue can vary from 1 to 100 calls. You set the length of the queue when you administer the RLT group.

Backup service provides for all CAS calls to be sent to a backup extension in the branch if:

- All RLTs maintenance-busy
- All RLTs are out of service
- The attendant presses a **Backup** button that is not lit

To activate this feature and to provide notification that backup service is in effect, assign the backup extension to a **Backup** button and an associated status lamp.

- The status lamp remains lit as long as backup service is in effect.
- To deactivate the CAS feature, the attendant presses the **Backup** button while the status lamp is lit. The system does not send calls to the backup extension unless all RLTs are maintenance-busy, or out of service.

The attendant can put a CAS call from a branch on Remote Hold. The branch holds the call, and drops the RLT. After a timeout, which is the same as the timed reminder for an attendant-held call, the branch automatically attempts to route the call back to the attendant. The returning call can queue for the RLT. Attendants can use Remote Hold when the attendant must put a call on hold to prevent the unnecessary use of RLTs.

Centralized Attendant Service (CAS) supports the following capabilities:

- Branch-generated call identification tones on page 554

Branch-generated call identification tones

The branch in a CAS network generates call identification tones, and transmits the tones to the CAS attendant through RLTs. These tones indicate the type of call from the branch, or the status of a call extended to or held at the branch. The attendant hears these tones in the console handset before the attendant is connected to the caller.

The following identification tones might vary by country.

- Incoming trunk calls: 480 Hz (100 ms), 440 Hz (100 ms), 480 Hz (100 ms) in sequence. The attendant hears this tone immediately after the attendant lifts the handset.
- Calls from a branch telephone to the main attendant, or calls that are transferred by a branch telephone to the main attendant 440 Hz (100 ms), silence (100 ms), 440 Hz (100 ms) in sequence. The attendant hears this tone immediately after the attendant lifts the handset.
- Calls that the system extends to an idle telephone, or recall on Does Not Answer: The attendant hears ringback tone (300 ms), and then connection to the normal ringing cycle.
- Calls that the system extends to a busy telephone, automatically waiting, or recall on Attendant Call Waiting: 440 Hz (100 ms).
- Calls that the system extends to a busy telephone, waiting denied, or not provided: A busy tone.
- Remote Hold or Remote Hold recall: A series of four to six cycles of 440 Hz (50 ms), and then silence (50 ms).
- Recall on Does Not Answer: A burst of ringback tones (300 ms), and then connection to normal ringback at any point in the cycle.
- Recall from a call that is on Remote Hold: A series of four to six cycles of 440 Hz (50 ms), and then silence (50 ms).
- Recall from a call that is waiting at a single line telephone: A burst of 440 Hz (100 ms).

The centralized attendant at the main location has access, through RLTs, to all outgoing trunk facilities at the branches in a CAS network. To extend an incoming LDN call to an outgoing trunk

at a branch, an attendant can dial the access code and then allow the caller to dial the rest of the number. The attendant can also dial the complete outgoing number.

Calls that are extended to busy single-line telephones at the branch wait automatically. If a call is in queue, the user hears a busy signal. When Station Hunting and Send All Calls is administered, the system routes the call along the administered path. If any extended call is waiting, and is unanswered within an administered interval, the branch system returns the call to the attendant. Call Waiting does not apply to multiappearance telephones. If no appearances are available, busy tone is sent to the attendant, who tells the caller that the line is busy.

The system also routes calls from telephones at the branch to an attendant over RLTs that are seized by the branch system. To reach the attendant, a branch caller dials the attendant-group access code. This access code is administrable. The default is 0. The conversation between the branch caller and the attendant ties up the seized RLT, but calls of this type are usually short.

Centralized Attendant Service administration

This section describes the prerequisites and the screens for the Centralized Attendant Service feature.

Preparing to administer Centralized Attendant Service

Procedure

1. Set up the attendant console.

   For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

2. Type `display system-parameters customer-options`. Press `Enter`.

3. On the Optional Features screen, ensure that the **Async.Transfer Mode (ATM) PNC** field is set to y.

   If this field is set to n, go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Centralized Attendant Service, or to open a service request.

   .

Screens for administering Centralized Attendant Service

Screen name	Purpose	Fields
Optional Features	Enable port network connectivity (PNC).	Async. Transfer Mode (ATM) PNC

Table continues…

Screen name	Purpose	Fields
Attendant Console	Assign feature buttons.	Any available button field in the **Feature Button Assignments** area.
Console-Parameters	Set up parameters for CAS.	• CAS • RLT Trunk Group Number • Timed Reminder on Hold • Return Call TImeout (sec)
Station	On a multiappearance telephone, assign feature buttons.	Any available button field in the **Feature Button Assignments** area.
Trunk Group	Set up a release link trunk (RLT) group.	All
Feature Access Code (FAC)	Set up a Feature Access Code (FAC) for CAS Remote Hold.	CAS Remote Hold/Answer Hold-Unhold Access Code

Considerations for Centralized Attendant Service

This section provides information about how the Centralized Attendant Service (CAS) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Centralized Attendant Service (CAS) under all conditions. The following considerations apply to Centralized Attendant Service (CAS):

- In a CAS network, systems can function either as branches or as the main location. A branch can connect to only one main location.
- CAS reduces the number of attendants that are required at a branch. For example, a chain of department stores can have a centralized attendant at the main store to handle calls for all of the branch stores.
- A branch can have an attendant. Access to the branch attendant must be by way of an individual attendant extension. Incoming trunk calls in a CAS network can bypass branch attendants. The centralized attendant can route these incoming trunk calls back to the branch attendant.
- Branch calls terminate on the CAS main system based day-destination or night-service destination of the incoming RLT trunk group. An attendant console might not always answer or extend incoming CAS calls.

  If someone other than an attendant answers a CAS call, that person can either press the **Flash** button on a multiappearance telephone, or flash the switch hook on a single-line telephone, to extend the call back to the branch. The branch reaction to flash signals and the branch application of tones is the same whether an attendant, or someone other than an attendant, answers or extends the call.
- If an extended call returns unanswered to the main attendant, the called party at the branch does not drop. The called party at the branch continues to be alerted until the caller releases.

Using this process, the attendant can talk to the caller, and then extend the call again, if the caller wants, without redialing the number.

- If an extended CAS call recall times out and goes to coverage, but is unanswered, the branch leaves the extended-to party ringing. The system drops coverage.
- When an analog telephone call goes to coverage, the call is dropped. This process is the exception to the branch leaving the extended-to party ringing. If the main attendant extends a call to an analog telephone, and that call goes to coverage and later returns to the main attendant, the call is treated as an incoming LDN call. If the user requests, the attendant must extend the call again.
- On an incoming CAS call to the main attendant, the system displays the **Name** field from the Trunk Group screen for that RLT to the attendant. Therefore, you must administer the **Name** field on the Trunk Group screen to provide meaningful branch identification information.
- The Music-on-Hold feature at a branch applies to two stages of LDN calls: during call extension, and when the call is on Remote Hold.

Interactions for Centralized Attendant Service

This section provides information about how the Centralized Attendant Service (CAS) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Centralized Attendant Service (CAS) in any feature configuration.

Abbreviated Dialing

The main attendant can use an Abbreviated Dialing button to extend CAS calls after the attendant obtains branch dial tone.

Attendant Auto-Manual Splitting

The Split lamp and button do not function on CAS calls to the main location that are extended through RLTs. Attendant conference does not function on CAS calls.

Attendant Control of Trunk Group Access

If a branch attendant has control of an outgoing RLT trunk group, the system routes new attendant-seeking calls to the branch attendant.

Attendant Override of Diversion

Use Attendant Override of Diversion with CAS.

Attendant Serial Calling

Attendant Serial Calling does not work for CAS calls.

Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS)

You can use AAR and ARS to route CAS calls.

Automatic Circuit Assurance (ACA)

When CAS is activated, the **ACA Referral Calls** field on the Feature-Related System Parameters screen must be set to local. The system interprets a referral destination of 0 as the local attendant,

if a local attendant exists. The CAS attendant cannot activate or deactivate ACA referral calls at a branch location.

Busy indicators can identify incoming calls over an RLT. You can also use Busy indicators to dial after the attendant starts to extend a call.

Busy-Indicator Buttons

Call Coverage

Use Call Coverage to redirect calls to a centralized attendant. Do not redirect calls to a CAS backup extension for backup service through Send All Calls to the coverage path of the backup extension.

Call Detail Recording (CDR)

If the CAS main RLT has the CDR option selected, the system generates CDR records for incoming CAS calls.

Call Forwarding

Do not forward calls to a CAS extension.

Call Park

If a CAS attendant parks a call and the call returns to the attendant after the Call Park expiration interval, the attendant hears incoming trunk-call notification.

Class of Restriction (COR)

Since COR information is not passed over RLTs, fully restricted service supports all CAS calls. Therefore, the system can use CAS to complete a public network call to a fully restricted telephone.

Distributed Communications System (DCS) operation

If an RLT trunk group is administered as a DCS trunk, the DCS message displays instead of the name of the incoming RLT trunk group on an incoming CAS call to the attendant. When the attendant answers the call, the attendant hears call identification tones. These tones indicate that the call is a CAS call. The attendant must use a **Trunk-Name** button to obtain the name of the RLT trunk group.

DXS and DTGS Buttons

DXS and **DTGS** buttons at the main attendant console can be used with CAS. With the **DXS** button, the attendant hears ringback tone after a delay of a few seconds.

Emergency Access to the Attendant

For CAS Branch Emergency Access calls that generate by a Feature Access Code, the system routes Off-Hook Alert to the branch attendant group. If there is no attendant in the branch, the system routes the call to the administered Emergency Access Redirection Extension of the branch. When the branch system is in CAS Backup Service, the system routes the calls to the backup telephone. The call is treated as a normal call.

Extending a CAS call by a nonattendant

CAS branch calls terminate at the CAS main location, based on the day-destination or the night-service destination of the incoming RLT trunk group. You can also answer a CAS call with the TAAS feature.

Usually, a nonattendant presses the **Flash** button to extend a CAS call. However, if the nonattendant does not have a **Flash** button, a nonattendant can extend the call in one of the following ways:

- Multiappearance telephone users can press the **Conference** or **Transfer** button, and then dial the extension. To complete the call, the user drops the call. To drop the extended-to party, the user presses the **Conference** or **Transfer** button again.
- Single line telephone users can flash the switch hook, and then dial the extension. To complete the call, the user drops the call. To drop the extended-to party, the user flashes the switch hook again.

Holding a CAS call by a nonattendant

A nonattendant with a multiappearance telephone can press the Hold button to hold a CAS call.

Hunt Groups

If the system directs an incoming CAS call to a hunt group, the system does not redirect the call to the coverage path of the hunt group. Depending on the circumstances, the attendant can get a busy tone or ringing.

Last Number Dialed (LND)

An attendant cannot extend calls with the LND feature.

Leave Word Calling (LWC)

If a message is left for a branch user, and the attendant at the CAS system tries to retrieve the message, permission is denied.

Night Service, Night Console Service

When the attendant places the CAS main location in Night Service, CAS calls terminate at the CAS main night-service destination. When an attendant places a branch location in Night Service, the system routes the CAS calls to the branch night console, to the LDN night telephone, or to the TAAS telephone.

Night Service, Trunk Answer from Any Station (TAAS)

In a multisystem DCS environment with CAS, transferring incoming trunk calls through Night Service Extension or TAAS varies. Such a transfer depends on the:

- Home system of the transferred-to telephone
- Home system of the connected trunk
- Type of night-service function that is chosen. The type of night-service function can be Night Service Extension, TAAS, or both Night Service Extension and TAAS.

Nonattendant. Display Trunk Name

If a nonattendant with a display telephone presses the **Trunk Name** button while the nonattendant is active on a trunk call, the system displays the value in the **Name** field from the Trunk Group screen.

QSIG CAS

The QSIG CAS service is not provided through the RLT trunks, as the QSIG CAS service is administered when the **Centralized Attendant** field is set to y on the QSIG Optional Feature screen.

Releasing a CAS call by a nonattendant

A nonattendant can drop the RLT by going on-hook, and then use the Disconnect or Drop button. A nonattendant can also drop the RLT by selecting another call appearance.

Security Violation Notification (SVN)

CAS attendants cannot receive referral calls from branch locations.

Timed Reminder

You can set the timer value for recalling held calls at the attendant console on the Console screen.

If an attendant at the CAS main location transfers a call from a branch to an extension at the main location, the timed reminder does not apply. The call does not return to the attendant if unanswered. If a branch call is unanswered, the branch timed reminder times out, and the system routes the call to a new RLT trunk, and back to a CAS main attendant.

Trunk-Name button

Use the **Trunk-Name** button when you make an outgoing call over a trunk that is administered to have no outgoing display.

Chapter 62: Class of Restriction

Use the Class of Restriction (COR) feature to:

- Define different levels of call origination and termination privileges
- Apply administration settings to objects that share the same COR number
- Identify what CORs can be service observed, and what CORs can be a service observer

Detailed description of Class of Restriction

You can use CORs to restrict communication between point A and point B. For example, a user tries to establish a communication path between point A and point B. The system checks whether the CORs have permission to communicate with one another. If the CORs have permission, the system completes the call. If the CORs do not have permission, the system does not complete the call. You control the level of restriction that the COR provides.

CORs also have other applications. You can apply administration settings to a COR, and then assign that COR to objects or facilities in the system. This use of CORs makes it easier to administer functions across a wide range of objects. CORs are assigned to a variety of objects, such as:

- Telephones
- Trunks
- Agent login IDs
- Data modules

Finally, you can set up CORs that are service observing and service observed. You can assign a COR to be a service observer. Then you identify what other CORs that the user can observe. You can also set up a COR to be serviced observed.

Note:

Your system might use only one COR or as many as necessary to control calling privileges.

Many objects can share the same COR number. You must administer a COR for the following objects:

- Agent login IDs

- Access endpoints
- Announcements and audio sources
- Attendant consoles
- Authorization codes
- Console parameters
- Hunt groups
- Loudspeaker paging
- Data modules
- Remote access (each barrier code has a COR)
- Telephones
- Terminating Extension Groups (TEGs)
- Trunk groups
- Vector Directory Numbers (VDNs

Note:

The **Outgoing Trunk Disconnect Timer (minutes)** field on the Class of Restriction screen provides the capability to disconnect an outgoing trunk automatically after an administrable amount of time. This field defaults to blank (outgoing trunk calls are only disconnected when dropped by one or all parties), or you can enter a timer value in number of minutes to apply to outgoing trunk calls if the initiating party belongs to this COR. For more information on values for the fields, see *Administering Avaya Aura® Communication Manager*.

Mask CLI/Station Name for Internal Calls

A typical Communication Manager internal call generally provides calling/called party numbers and administered text name string, which are displayed on the involved parties' terminals.

Beginning with Communication Manager Release 4.0, the Mask CLI/Station Name for Internal Calls feature provides a new station capability (through proper COR administration) of masking off such information and replacing it with a hard-coded, system-wide text string, Info Restricted, which will be displayed on the party's terminal. In addition, the feature shall provide a means of administering that the CPN/Name information not be masked-off when the call is made.

Currently Communication Manager can block calling party number and name to be sent to the network with proper trunk/station administration.

This new feature, Mask CLI/Station Name for Internal Calls takes a similar approach to these existing Communication Manager capabilities whenever it is applicable for internal calls.

The Class of Restriction screen has a new field called **Mask CPN/NAME for Internal Calls**. Enter y to hide the display of calling/called party numbers and administered name on internal calls. The Class of Service screen also has a new field called **Masking CPN/Name Override**. Users can set this field to y to override the Mask CLI/Station Name for Internal Calls capability.

For more information on these fields, see *Avaya Aura® Communication Manager Screen Reference*.

Strategy for assigning CORs

When you administer your system, the best strategy is to assign CORs to similar groups or objects. For example, you might create a unique COR for each type of user or facility, such as:

- Call center agents
- Account executives
- Supervisors
- Administrative assistants
- Paging zones
- Data modules

You might also want to create a unique COR for each type of restriction.

You can assign the same COR to more than one object. Objects with the same COR might be similar objects, such as two telephones, or different objects, such as a telephone and a trunk group.

To enhance your system security, you can:

- Assign a separate COR to incoming trunk groups and outgoing trunk groups, and then restrict calls between the two groups.
- Set appropriate calling party restrictions and Facility Restriction Levels (FRLs) to limit the calling permissions as much as possible.

Types of restrictions

Calling party restrictions

Calling party restrictions define the privileges for telephones that make outbound calls. If you do not need to restrict telephones that make outbound calls, assign a COR with the **Calling Party Restriction** field set to none.

You can use calling party restrictionsfor:

- Unrestricted telephones
- Trunk groups
- Terminating Extension Groups (TEGs)
- Uniform Call Distribution (UCD) groups
- Direct Department Calling (DDC) groups
- Data modules
- Attendant groups

- Individual attendant extensions

All-Toll restrictions and TAC-Toll restrictions

Toll restrictions prevent users from placing public network calls to certain toll-call numbers. You assign toll restrictions to outgoing trunk groups on the Trunk Group screen. You disable Trunk Access Code (TAC)-toll restrictions for specific outgoing trunk groups on the Trunk Group screen.

Origination restrictions

You can use origination restrictions to prohibit users from originating calls. These users can still receive calls.

Outward restrictions

You can use outward restrictions to prevent users from placing calls to the public network. These users can still place calls to other telephone users, to the attendant, and over tie trunks. If necessary, an attendant or an unrestricted telephone user can extend a call to an outside number for an outward-restricted telephone user.

Calls that come into a trunk are denied if the:

- **Calling Party Restriction** field on the Class of Restriction screen is set to outward
- Calls use the Automatic Alternate Routing (AAR) or the Automatic Route Selection (ARS) feature

Called party restrictions

Called party restrictions define the privileges for telephones that receive inbound calls. If you do not need to restrict telephones that receive inbound calls, assign a COR with the **Called Party Restriction** field set to none.

You can use called party restrictions for:

- Unrestricted telephones
- Trunk groups
- Terminating Extension Groups (TEGs)
- Uniform Call Distribution (UCD) groups
- Direct Department Calling (DDC) groups
- Data modules
- Attendant groups
- Individual attendant extensions

Even if the system redirects a call from one telephone to another, the system checks for called party restrictions only at the called telephone. For example, if a called telephone with no restrictions activates the Call Forwarding feature to a restricted telephone, the system still completes the call.

Inward restrictions

To receive only internal calls, you can use inward restrictions. With inward restrictions, users at assigned telephones cannot receive:

- Public network calls
- Attendant originated calls
- Attendant extended calls

The system checks only the COR of the originally called telephone, unless you administer a three-way COR on conference calls and transfer calls. The system routes denied calls to:

- Intercept tone
- A recorded announcement
- The attendant, for Direct Inward Dialing (DID) calls

Manual terminating line restrictions

To receive calls only from an attendant, users can use manual terminating line restrictions. The system can redirect calls to a telephone with manual terminating line restrictions. The system checks only the COR of the originally called telephone.

The system routes the following calls to the attendant:

- Local central office (CO) calls
- Foreign exchange (FX) calls

The system redirects Direct Inward Dialing (DID) calls to:

- Intercept tone
- A recorded announcement
- The attendant

Public restrictions

Public restrictions prohibit users from receiving public network calls. The system routes denied calls to:

- Intercept tone
- A recorded announcement
- The attendant

Using Public restrictions, users can still receive internal calls from other telephones, or calls that are extended from the attendant.

Termination restrictions

You can use termination restrictions to prohibit users from receiving any calls. These users can still originate calls. The system routes DID or Advanced Private-Line Termination calls to a recorded announcement or to the attendant.

Fully restricted service

With fully restricted service, users cannot make or receive public network calls. Users who have fully restricted service cannot use authorization codes to deactivate this feature.

COR-to-COR restrictions

You can restrict calls from one COR to another COR. You can use COR-to-COR calling restrictions to prohibit user access to specific telephones or specific trunk groups, such as CO trunk groups. Any or all trunk groups can be in a trunk-restriction COR. The system routes restricted calls to intercept tone.

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 (FRLs) to block groups of users from accessing specific trunk groups.

Class of Restriction administration

The following steps are part of the administration process for the Class of Restriction (COR) feature:

- Displaying administered CORs
- Setting up a COR
- Allowing users to change their own COR

Related links

Displaying administered CORs on page 567
Setting up a COR on page 567
Allowing users to change their own COR on page 568

Screens for administering Class of Restriction

Screen name	Purpose	Fields
Class of Restriction Information	List what CORs are administered on your system.	All

Table continues…

Screen name	Purpose	Fields
Class of Restriction	• Apply administration settings to all objects that share the same COR number. • Restrict the types of calls that a user can make and receive. • Identify what CORs can be service observed, or be a service observer.	All
Optional Features	Ensure that users can change their own COR without assistance from an administrator.	Change COR by FAC
Feature Access Code (FAC)	Assign a Feature Access Code (FAC) so that the user can change their own COR without assistance from an administrator.	Change COR Access Code
Feature-Related System Parameters	Assign a password that is required before a user can change their own COR.	Password to Change COR by FAC

Displaying administered CORs

Procedure

1. Type `list cor`. Press `Enter`.
2. On the Class of Restriction Information screen, click **Next** continually to see all the CORs.
3. After you review this information, press **Cancel**.

Setting up a COR

Procedure

1. Type `change cor n`, where *n* is the number of a specific COR. Press `Enter`.

   The system displays the Class of Restriction screen.
2. In the **COR Description** field, type a name for this COR.

   Assign a name for the COR that clearly reflects either the purpose or the members of the COR.
3. Complete all the applicable fields on page 1 of this screen.

   Specifically, you must:

   - Right-click the **Calling Party Restriction** field to see a list of options. Select an appropriate item from the list.
   - Right-click the **Called Party Restriction** field to see a list of options. Select an appropriate item from the list.

4. Press `Enter` to save your changes.
5. Click **Next** to see the next screen.
6. Complete all the applicable fields on page 2 of this screen.
7. Press `Enter` to save your changes.
8. Click **Next** to see the next screen.

   The numbers represent the available CORs. All fields default to y.
9. To restrict a user who is assigned this COR from calling someone in another COR, change the Calling Permission of the COR number to `n`.
10. Press `Enter` to save your changes.
11. Click **Next** to see the last screen.

    The numbers represent the available CORs. All fields default to y. Complete this screen only if you set the **Can Be A Service Observer** field on page 1 to y. If the **Can Be A Service Observer** field is set to n, you can skip this screen.

    If a specified COR is set to y, but the **Can Be Service Observed** field on page 1 of that COR is set to n, that COR cannot be service observed.
12. To indicate what COR cannot be service observed, change the value of the COR number to `n`.

    In this example, a user who is assigned COR 10 cannot service observe a user who is assigned COR 19.
13. Press `Enter` to save your changes.

Allowing users to change their own COR

You can allow users to change their own COR from the telephone through a Feature Access Code (FAC). Users can change from the existing COR to any other COR. To restrict this feature, you can also require that users enter a password before the users can change their own COR.

Note:

Administrators can also allow users to change only between two predetermined CORs. For more information, see the Station Lock feature.

Prerequisites

You must complete the following actions before you can allow users to change their own COR:

- On the Optional Features screen, ensure that the **Change COR by FAC** field is set to y. If this field is not set to y, users cannot change their own COR. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to COR, or to open a service request.

  To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

To allow users to change their own COR to any other COR, you must complete the following procedures:

1. Assign a FAC for changing the COR.
2. Assign a password users enter to change the COR.

Assigning a FAC for COR change

Procedure

1. Type `change feature-access-codes` and press `Enter`.

   Communication Manager displays the Feature Access Code (FAC) screen.
2. In the **Change COR Access Code** field, type an FAC that conforms to your dial plan.
3. Press `Enter` to save your changes.
4. Ensure that you notify all users of the assigned FAC.

Assigning a password for COR change

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. On the Feature-Related System Parameters screen, click `Next` until you see the **Password to Change COR by FAC** field.
3. In the **Password to Change COR by FAC** field, type a password.

   This field determines if Communication Manager requires the user to enter a password when the user tries to change the COR, and what that password is.
4. Press `Enter` to save your changes.
5. Ensure that you notify all users of the assigned password.

End-user procedures for Class of Restriction

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Changing a COR with a FAC

Procedure

1. Dial the Change COR Access Code FAC.
2. Dial the password to change a COR, followed by #.
3. Enter the extension of the station to change the COR.
4. Enter the new 3-digit COR followed by `#`.

For example, if the new COR is 19, enter `019#`.

Note:

- You can invoke this feature from a station with Console Permissions enabled in its Class of Service (COS) only.
- You cannot assign a 4-digit COR value to a station.

Interactions for Class of Restriction

This section provides information about how the Class of Restriction feature interacts with other features in your system. Use this information to ensure that you receive the maximum benefits of the Class of Restriction in any feature configuration.

Automatic Alternate Routing (AAR) or Automatic Route Selection (ARS)

Termination and miscellaneous restrictions do not apply to AAR or ARS calls. AAR or ARS access to a trunk group overrides miscellaneous trunk restrictions.

AAR or ARS Partitioning

Use a COR to assign partition group numbers.

Abbreviated Dialing

Communication Manager does not check direct calls that are made from group lists. These lists are inaccessible to a user whose telephone is fully restricted. However, after a user calls from the Abbreviated Dialing group list, the system checks all subsequent transfer and conference attempts.

Abbreviated Dialing Privileged Group Number List

A telephone user with authorization to access an Abbreviated Dialing Privileged Group Number List can place calls to any number on that list. The system does not check COR assignments.

Bridged Call Appearance

A COR assigned to a telephone also applies to calls that originate from a bridged call appearance of that telephone.

Call Coverage

Users who are restricted from calls can still receive calls that Call Coverage directs to these users. When a call goes to coverage, the system uses the restrictions of the called party, not of the covering party. When a call is redirected to coverage, the system does not check the COR of the covering party. If the COR of the covering party is fully restricted, the system cannot complete the call.

Call Forwarding All Calls

If a COR restricts a call between the forwarding extension and the forwarded-to extensions, Call Forwarding is denied. The system always checks when Call Forwarding is activated, but not when the system forwards a call.

Call Vectoring

When the system directs a call to a vector directory number (VDN), the system compares the COR of the caller and the VDN. This comparison determines if the caller can access the associated call vector.

Centralized Attendant Service (CAS)

Since COR information is not passed over release link trunks (RLT), fully restricted service allows all CAS calls. Therefore, using CAS, a public network call can be completed to a fully restricted telephone.

Class of Restriction Display to the Attendant

The attendant can display the COR for each telephone.

Class of Service (COS)

In some cases, the COS of a user can override a COR. For more information, see the **Trk-to-Trk Restriction Override** field in the Class of Service feature description.

Controlled Restriction

Restrictions that you assign through Controlled Restriction override any COR restrictions.

Distributed Communications System (DCS)

Fully restricted service allows all DCS calls. Using DCS, a public network call can be completed to a fully restricted telephone.

Emergency Access to Attendant

A COR supports Emergency Access to Attendant calls.

Fully Restricted Service

Do not assign fully restricted service to a telephone that has these features or conditions:

- Abbreviated Dialing
- Bridged Call Appearance
- Attendant telephones
- Night Service telephones
- Telephones that are Call Coverage or Send All Calls points
- Telephones that are Call Forward destinations
- Telephones that are Call Pickup points

Hunt Groups

The system checks the COR that is assigned to a hunt group on calls that are redirected by the Direct Department Calling (DDC) or Uniform Call Distribution (UCD) of the hunt group. If the COR of the hunt group does not have fully restricted service, extensions in the hunt group can receive calls from the public network.

Night Service and Night Station Trunk Answer From Any Station

Both the Night Service feature and the Night Station Trunk Answer From Any Station feature override:

- Inward restrictions
- Manual terminating line restrictions
- Public restrictions

Personal Central Office Line (PCOL)

Do not assign fully restricted service to users who have a personal central office line. If you do, you are paying for a CO line that no one can use.

Power Failure Transfer

All authorization features are bypassed when the system is in emergency transfer mode.

Privileged System Number List

A telephone user with authorization to access a Privileged System Number List can place calls to any number on that list. The system does not check COR assignments.

Remote Access

If the user enters a barrier code during connection to remote access, the system uses the COR that is associated with that code for authorization checks. If remote access does not require a barrier code, the system uses the COR of the default barrier code. Remote access can require an authorization code instead of, or in addition to, the barrier code. If the system requires an authorization code, the COR of the authorization code overrides the COR of the barrier code.

Tie trunk access

The system can complete incoming dial-repeating tie trunk calls directly to an inward-restricted telephone or a public-restricted telephone. An attendant cannot extend incoming dial-repeating tie trunk calls to an inward-restricted telephone.

Transfer

When you administer a three-way conference, a user cannot transfer incoming trunk calls to an inward-restricted telephone. Transferred calls are subject to three-way COR Checking restrictions.

A user can transfer incoming trunk calls from an unrestricted telephone to an inward-restricted telephone or a public-restricted telephone. However, you must override the three-way conference COR.

Chapter 63: Class of Service

Use the Class of Service (COS) feature to allow or deny user access to some system features.

Detailed description of Class of Service

Use the COS feature to allow or deny user access to some system features, such as:

- Automatic Callback
- Call Forwarding
- Data Privacy
- Trunk-to-Trunk Transfer Override
- QSIG Call Offer Originations
- Contact Closure Activation
- Console Permission

Use the Class of Restriction (COR) feature, instead of COS, to define the restrictions that apply when a user places or receives a call. For more information, see the Class of Restriction feature.

COS does not apply to trunk groups, except for the Remote Access feature. For more information, see the Remote Access feature.

Class of Service administration

The following steps are part of the administration process for the Class of Service feature (COS):

- Defining COS for your system
- Assigning a COS

Related links

Defining COS for your system on page 574
Assigning a COS on page 577

Screens for administering Class of Service

Screen name	Purpose	Fields
Attendant Console	Assign Class of Service (COS) for the attendant.	COS
Class of Service	Define COS for your system.	All
Console-Parameters	Assign COS for all the attendant consoles.	COS
Data Modules	Assign COS for a data module.	COS
Remote Access	Assign the COS associated with the barrier code of the Remote Access extension.	COS
Station	Assign COS for a user.	COS

Defining COS for your system

Procedure

1. Type `change cos`. Press `Enter`.

   The system displays the Class of Service screen.

2. Perform one of the following actions for any, or all, of the COSs, which are numbered zero through 15:

   - If you want to activate the feature for the COS, type `y`.
   - If you do not want to activate the feature for the COS, type `n`.

3. Press `Enter` to save your changes.

Descriptions of the COS features

The system displays some features only if the associated feature is set to y on the Feature-Related System Parameters screen.

- Automatic Callback

  A user can request Automatic Callback. For more information, see the Automatic Callback feature.

- Automatic Exclusion

  A user can automatically activate Privacy Exclusion when the user goes off hook at a telephone that has an assigned **Exclusion** button.

  If you set this field to n, the user can use manual exclusion when the user presses the Exclusion button, either before the user dials a call or during a call.

  The system displays this field when the **Automatic Exclusion by COS** field on the Feature-Related System Parameters screen is set to y.

- Call Forwarding All Calls

A user can forward all calls to any extension. For more information, see the Call Forwarding feature.

- Call Forwarding Busy/DA

  The system can forward calls when the user is active on a call, or does not answer a call. For more information, see the Call Forwarding feature.

- Client Room

  Users can access the Check-In, Check-Out, Room Change/Swap, and Maid status functions. In addition, Client Room is required at consoles or telephones that are to receive message-waiting notification.

  You can administer a COS for Client Room only when you have Hospitality Services and a Property Management System (PMS) interface. See the *GuestWorks® and DEFINITY® Systems Technician Handbook for Hospitality Installations* for more information.

- Console Permissions

  A user having a multiappearance telephone can use Console Permissions, to control the same features that the attendant controls. You might assign this permission to front-desk personnel in a hotel or a motel, or to a call center supervisor. With console permission, a user can:

  - Activate Automatic Wakeup for another extension
  - Activate and deactivate controlled restrictions for another extension, or group of extensions
  - Activate and deactivate Do Not Disturb for another extension, or group of extensions
  - Activate Call Forwarding for another extension
  - Add and remove agent skills
  - Record integrated announcements

- Data Privacy

  A user can enter a Feature Access Code (FAC) to protect a data call from interruption by any of the system override or ringing features. For more information, see the Privacy feature.

- Extended Forwarding All

  A user can use Call Forwarding All Calls from an off-site telephone.

  You can change a COS to y, only if the **Extended Cvg/Fwd Admin** field on the System Parameters Customer-Options screen is set to y. For more information, see the Extended User Administration of Redirected Calls feature.

- Extended Forwarding B/DA

  A user can activate Call Forwarding from an off-site telephone.

  You can change a COS to y only if the **Extended Cvg/Fwd Admin** field on the System Parameters Customer-Options screen is set to y. For more information, see the Extended User Administration of Redirected Calls feature.

- Off-Hook Alert

  You can change a COS to y, only if either the **Hospitality (Basic)** field or the **Emergency Access to Attendant** field on the System Parameters Customer-Options screen is set to y. For more information, see the Emergency Access to Attendant feature.

- Personal Station Access (PSA)

  A user can use a FAC to associate a telephone to the extension that is assigned to the user.

  You must set this field to n for virtual telephones.

  You can change this field to y, only if the **Personal Station Access (PSA)** field on the Optional Features screen is set to y. For more information, see the Personal Station Access feature.

- Priority Calling

  A user can dial a FAC to originate a priority call. For more information, see the Priority Calling feature.

- QSIG Call Offer Originations

  A user can invoke QSIG Call Offer services. For more information, see *Administering Network Connectivity on Avaya Aura® Communication Manager*.

- Restrict Call Fwd-Off Net

  If you set this field to y, a user cannot forward calls to the public network.

  For security reasons, type y in the **Restrict Call Fwd-Off Net** field for all COS, except those that you use for special circumstances. For more information, see the Call Forwarding feature.

- Trk-to-Trk Restriction Override

  Security alert:

  You increase the risk of toll fraud if you allow users to perform trunk-to-trunk transfers.

  A user can override any system COR-to-COR calling party restrictions that would otherwise prohibit the trunk-to-trunk transfer operation for a user with this COS. For more information, see the Transfer feature.

From Communication Manager, Release 3.0, the Class of Service screen has a new field **VIP Caller**. The **VIP Caller** field enables automatic priority calling to extensions when it is marked y on the Class of Service screen. The default for this field is n.

For more information on impact of this field on Priority Calling, see the feature description on Priority Calling.

Assigning a COS

Procedure

1. Change the **COS** field on any of the following screens:
   - Attendant Console
   - Console-Parameters
   - Data Modules
   - Remote Access
   - Station
2. Press `Enter` to save your changes.

Considerations for Class of Service

This section provides information about how the Class of Service feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Class of Service under all conditions. The following considerations apply to Class of Service:

Hunt Groups

Many Hunt Groups have a COS of 1. Ensure that you do not cause unintended restrictions for Hunt Groups when you administer COS 1.

Interactions for Class of Service

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

- Class of Service (COS) controls use of the following features and capabilities:
  - Automatic Callback
  - Automatic Exclusion
  - Call Forwarding
  - Call Forward Busy/Don’t Answer
  - Client room
  - Console permission
  - Data Privacy

- Extended Forwarding All
- Extended Forwarding Busy/Don’t Answer
- Off-hook alert
- Personal Station Access
- Priority Calling
- QSIG Call Offer Originations
- Restrict Call Forwarding Off-Net
- Trunk-to-Trunk Transfer Restriction Override

Chapter 64: Clock Synchronization over IP

When traditional synchronization is unavailable, you can use the Clock Synchronization over IP (CSoIP) feature. You can use this feature on G450 and G430 gateways to provide system clocking across IP networks.

Detailed description of Clock Synchronization over IP

Communication Manager creates Inter-Gateway Connections (IGCs) to convey the IP streams. The G450 and G430 Branch Gateways provide both source ports and sync ports for the IGCs. CSoIP supports TDM-based devices, such as an H.320 video device to retain and transmit within an IP infrastructure. You administer Clock Synchronization over IP through the Communication Manager's SAT Administration forms.

Instead of DS1 or BRI interface, you can use a local clock as the clocking source. You can choose a primary and any other backup sources.

The Communication Manager maintenance object and connection manager create and maintain the synchronization domains, also known as sync domains. A sync domain is a clock source that emanates IGC streams to clock receivers. All gateways involved with the CSoIP feature are referred to as members. A master domain is a clock source derived from a DS1 or BRI, which is used to emanate IGC streams to clock receivers. Other members that use the incoming IGC stream for internal clocking are known as slave clocks. The receiver is one hop level below the clock source. A secondary clock domain uses the incoming IGC stream, which is used to clock outgoing IGC streams to other members.

Depending on the limitation of the fan-out, a single clock source cannot source a stream to the maximum number of gateways. As a result, some clock receivers also become clocking source, known as the secondary clock source. These, in turn, constitute sync domains.

When the first IGC source comes into service, it becomes the default system clock source. All other IGC sources become slaves until the fan-out limit is reached. After the fan-out limit is reached, a slave is promoted to a secondary clock source, known as a tandem clock. Subsequent receivers are then clocked from the secondary source until its fan-out is reached. Then another slave from that sync domain is promoted to a tandem clock. This process takes place as each clock source reaches its fan-out limit.

When a master clock board comes into service, it is used to create a master clock domain if there is an IGC source board already providing IGC streams. The highest level clock source that was the default system clock source is demoted and becomes a receiver of a master clock source and

becomes a tandem clock. There can be as many master clock domains as there are administered sync sources.

The CSoIP feature does not attempt to mitigate the reference board outages. If such a board goes out of service, the traditional sync feature raises an alarm and you need to rectify the problem. Removing or adding any reference board from translations causes the CSoIP feature to adjust to move members to another source or begin adding members to the new source.

There can be several DS1s, BRIs, or other boards capable of providing a reference from the PSTN, and each can be used by the CSoIP feature to provide sync to a group of members.

Clock Synchronization over IP administration

The following tasks are part of the administration process for the CSoIP feature:

- Setting up IP synchronization
- Setting up IP synchronization for the gateway
- Setting up IP synchronization for the network region
- Assigning synchronization reference for the gateway
- Setting up the DS1 board as a synch Source reference
- Setting up the BRI trunk board as a Synch Source reference
- Disabling synchronization

For information on how to administer the above tasks, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Clock Synchronization over IP

Screen name	Purpose	Fields
Feature-Related System Parameters	Set up the Clock Synchronization over IP feature.	Synchronization over IP
Media Gateway	Set up IP synchronization on the gateway.	Use for IP Sync
IP Network Region	Set up IP synchronization on the network region.	Sync
IP Synchronization Source Media Gateway	Assign synchronization reference to the primary and secondary gateway.	Primary Secondary

Table continues…

Screen name	Purpose	Fields
DS1	Set up the DS1 board as a Synch Source.	For information on fields, see the Configuring a DS1 media module example section of *Administering Avaya Aura® Communication Manager*.
ISDN-BRI Trunk Media Module	Set up the BRI trunk board as a Synch Source.	Synch Source

Interactions for Clock Synchronization over IP

This section provides information about how the Clock Synchronization over IP (CSoIP) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of CSoIP in any feature configuration.

Survivable remote and survivable core servers

If a survivable remote and survivable core servers control the gateways with the primary and secondary synchronization source, the elements under the control of that survivable server have clock synchronization. If the primary and secondary synchronization source is not controlled by the survivable server in a failover fragment:

- The segment performs as if it had no primary or secondary source for clock synchronization.
- Any gateways with a DS1 or BRI interface in service takes its clock source from that DS1 or BRI interface.

Chapter 65: Conference

Use the Conference feature with the associated **Conf** button to create a conference without the assistance of an attendant.

Detailed description of Conference

Use the Conference feature, with the associated **conf** button, to create a conference without the assistance of an attendant.

A user with a multiple appearance telephone with a **conf** button can create a conference with as many as six participants. However, if the **12–party Conferences** field is enabled in the Feature-Related System Parameters screen, 12 parties can participate in a conference call.

A user with a single-line telephone can create a conference with as many as three participants. Each of these three participants can then add another participant. Thus, a user who has a single-line telephone can create a conference call with as many as six participants.

Note:

For 12 parties to participate in a conference, you must enable the **12–party Conferences** field in the Feature-Related System-Parameters screen.

Conference and DCP, hybrid, IP, wireless, and ISDN-BRI telephones

A user with a Digital Communications Protocol (DCP), hybrid, IP, wireless, or ISDN-BRI telephones can use the Conference feature for a call on hold when:

- Only one call is on hold
- No call appearances are active
- An available call appearance exists for the conference call

If more than one call is on hold, the user must make a call active to start a conference. If the user presses the **conf** button when two or more calls are on hold, the system ignores the conference request from the user.

If the user has an active call, and also has calls on hold, the system includes the active call in the conference when the user presses the **conf** button.

Meet-me Conference overview

Using the Meet-me Conference feature, users can set up a dial-in conference of up to six parties. The Meet-me Conference feature uses Call Vectoring to process the setup of the conference call. For more information, see the “Meet Me Conference” feature.

Note:

For 12 parties to participate in a Meet-me conference, you must enable the **12–party Conferences** field in the Feature-Related System-Parameters screen.

Conference/Transfer Toggle/Swap

A user who sets up a conference call can use the Conference/Transfer Toggle/Swap capability to talk back and forth between two users before the user connects all the participants to the conference call. The display also toggles between the two parties. The Conference/Transfer Toggle/Swap capability is unavailable on attendant consoles.

The user uses an administered feature button, toggle-swap, for the Conference/Transfer Toggle/Swap capability

No Dial Tone Conferencing

This capability eliminates the dial tone that the user usually hears while the user adds the participants to the conference call. A user uses the No Dial Tone Conferencing capability to add existing calls to a conference call. The user does not need to select a line appearance if there is someone on hold, or if the system is alerting a line appearance.

For example, a user places a call on hold, and talks to another party. When the user presses the **conf** button and then presses the button of the call on hold, the party on hold joins the conference without hearing a dial tone.

No Hold Conference

When a user who is active on a call creates a conference call, the user can use the No Hold Conference capability to add another participant to a conference call, while the user continues a conversation with the participant on the call that is currently active. When the user calls the new participant, the new participant automatically joins the conference when the new participant answers the call.

For example, a user presses the administered no-hld-cnf feature button and then dials an extension. The party that answers the call automatically joins the conference.

If the called user does not answer the call within the time that you specify in the **No Hold Conference Timeout** field on the Feature-Related System Parameters screen, the system deactivates the No Hold Conference capability for the call.

Users with multiline digital telephones can use the No Hold Conference capability.

Select Line Appearance Conferencing

If a user is at a call on line B, and another line is on hold or an incoming call alerts at line A, the user can press the **conf** button to bridge the calls together. If the user uses the select line appearance capability, the user can press a line appearance button to complete a conference instead of pressing the **conf** button a second time.

Selective Conference Party Display, Drop, and Mute

A user, who has a digital telephone with a display, or an attendant with an attendant console, can use the Selective Conference Party Display, Drop, and Mute capability to identify the participants on a call.

The conference prompts that the system displays are based on the user Class of Restriction (COR). The display prompts are based on the user COR, independent of the select line appearance conferencing and the No Dial Tone Conferencing capability. The display messages vary depending on the activation of the various Conference capabilities. The user COR controls the display of any additional information.

A user presses the administered conf-dsp feature button to scroll through the telephone numbers and names of the participants on the call. The telephone numbers of the participants are always available, although the names of the participants are sometimes unavailable. When the system displays the telephone number of a participant, the user can either press the administered fe-mute feature button to place the participant on mute, or the user can press the drop button to drop the participant from the call.

The ability to place a call participant on mute is useful when that participant has a noisy trunk line because of a cell phone, music-on-hold, or background noise. The Selective Conference Party Mute capability applies only to trunk lines, and a user can mute only one trunk line on a conference call.

Click to Conference

For the Click to Conference feature, make sure the **Enhanced Conferencing** field is set to y on the Optional Features screen.

Note:

For more information on how to administer the Click to Conference feature, see: *Installing, Administering, Maintaining, and Upgrading Avaya Aura® SIP Enablement Services.*

SIP Softphone Release 2.1 Quick Setup Guide, 16-600974

Conference administration

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

- Administering Conference feature parameters

- Assigning the togle-mute feature button
- Assigning Enhanced Conferencing feature buttons

Related links

Administering Conference feature parameters on page 585
Assigning the togle-swap feature button on page 587
Assigning Enhanced Conferencing feature buttons on page 587

Screens for administering Conference

Screen name	Purpose	Fields
Attendant Console	Assign conf-dsp, fe-mute, and togle-swap feature buttons to an attendant console	Any available button field in the **Feature Button Assignments** area
Feature-Related System Parameters	Aborts setting up a conference call when the phone disconnects	Abort Conference
	Specify that the system generate a conference tone	Conference Tone
	Specify the maximum number of participants in a conference call when any of the participants uses a public network trunk	Conference Parties With Public Network Trunks
	Specify the maximum number of participants on a conference call when none of the participants uses a public network trunk	Conference Parties Without Public Network Trunks
	Specify the number of seconds before the system deactivates the No Hold Conference capability for a call	No Hold Conference Timeout
	Specify that a user who is on hold hears dial tone while the conference owner adds another conference participant	No Dial Tone Conferencing
	Specify that the user can use the line appearance rather than the **Conf** button to include a call in a conference	Select Line Appearance Conferencing
Station	Assign conf-dsp, fe-mute, no-hold-conf, and togle-swap feature buttons to a user telephone	Any available button field in the **Button Assignments** area

Administering Conference feature parameters

About this task

Administer the Feature-Related System Parameters screen to support the Conference feature on your system.

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. **(Optional)** For 12-party conference, enable the **12-party conference** field.
3. On the Feature-Related System Parameters screen, click **Next** until you see the **Public Network Trunks on Conference Call** field.
4. In the **Public Network Trunks on Conference Call** field, type the maximum number of participants with public network trunks that you want to participate in a conference call.

   The valid entries for this field are 0 to 5, or 11.

   Type `0` if you do not want any public network trunks to participant in a conference call. If you type `0` in this field, the **Conference Parties with Public Network Trunks** field does not appear on the Feature-Related System Parameters screen.
5. In the **Conference Parties without Public Network Trunks** field, type the maximum number of participants without public network trunks that you want to participate in a conference call.

   The valid entries for this field are 3 to 6, or 12.
6. In the **Conference Tone** field, perform one of the following actions:
   - If you want the participants in a conference call to hear the conference tone if there are three or more participants on a conference call, type `y`.
   - If you do not want conference participants to hear the conference tone if there are three or more participants on a conference call, type `n`.
7. Click **Next** until you see the **No Dial Tone Conferencing** field.
8. In the **No Dial Tone Conferencing** field, take one of the following actions:
   - If you want a user who is on hold to hear dial tone while the conference owner adds another conference participant, type `n`.
   - If you do not want a user who is on hold to hear dial tone while the conference owner adds another conference participant, type `y`.
9. In the **Select Line Appearance Conferencing** field, take one of the following actions
   - Type `y` to activate select line appearance conferencing.
   - Type `n` to deactivate select line appearance conferencing.
10. In the **Abort Conference** field, perform one of the following actions:
    - If you want the user to stop a conference call if the user hangs up the telephone before the conference call is set up, type `y`.
    - If you do not want the user to stop a conference call when the user hangs up the telephone before the conference call is set up, type `n`.
11. In the **No Hold Conference Timeout** field, type the number of seconds that you want the system to wait while a user uses the No Hold Conference capability to add a participant to a conference call.

Note that you must set the **Answer Supervision** field on the Trunk Group screen to fewer seconds than the seconds in the **No Hold Conference Timeout** field.

12. Press `Enter` to save your changes.

Assigning the togle-swap feature button

Procedure

1. Type `change station` *n* and Press `Enter`.

   Where *n* is the extension to which you want to assign the Conference/Transfer Toggle/Swap capability.

2. On the Station screen, click `Next` until you see the **Button Assignments** area.
3. In the **Button Assignments** area, type `togle-swap` next to the button you want the user to use for the Conference/Transfer Toggle/Swap capability.
4. Press `Enter` to save your changes.

Assigning Enhanced Conferencing feature buttons

Before you begin

On the Optional Features screen, verify that the **Enhanced Conferencing** field is set to y, if you want to use the Selective Conference Party Display, Drop, and Mute capability and the No Hold Conference capability on your system. If the **Enhanced Conferencing** field is set to n, your system stops supporting the Selective Conference Party Display, Drop, and Mute capability. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to the Enhanced Conferencing feature, or to open a service request.

To view the Optional Features screen, enter `display system-parameters customer-options`.

Procedure

1. Assign a COR for the Selective Conference Party Display, Drop, and Mute capability.
2. Assign the **conf-dsp**, **fe-mute**, and **no-hld-cnf** feature buttons to a user.
3. Assign the **conf-dsp** and **fe-mute** feature buttons to an attendant.

Assigning the Enhanced Conference COR

Procedure

1. Type `change COR` *n*, where *n* is the number of the COR to which you want to assign the Selective Conference Party Display, Drop, and Mute capability. Press `Enter`.
2. On the Class of Restriction screen, click **Next** until you see the **Block Enhanced Conference/Transfer Displays?**.

3. In the **Block Enhanced Conference/Transfer Displays?** field, perform one of the following actions:
   - If you want the system to block all the enhanced conference/transfer display messages except “Transfer Completed” for a user or an attendant, type `y`.
   - If you do not want the system to block all the enhanced conference/transfer display messages except “Transfer Completed” for a user or an attendant, type `n`.

Assigning Enhanced Conferencing feature buttons to a user

Procedure

1. Type `change station n`, where *n* is the telephone number of the extension to which you want to assign the following capabilities:
   - Conference Display
   - Selective Conference Party Display, Drop, and Mute
   - No-Hold Conference

   Press `Enter`.
2. On the Station screen, click **Next** until you see the **Button Assignments** area.
3. In the **Button Assignments** area, perform the following actions:
   - Type `conf-dsp` next to the button that you want the user to use for the Conference Display capability.
   - Type `fe-mute` next to the button that you want the user to use for the Selective Conference Party Display, Drop, and Mute capability.
   - Type `no-hld-cnf` next to the button that you want the user to use for the No-Hold Conference capability.
4. Press `Enter` to save your changes.

Assigning Enhanced Conferencing feature buttons to an attendant

Procedure

1. Type `change attendant n`, where *n* is the number of the attendant console to which you want to assign the Conference Display capability, and the Selective Conference Party Display, Drop, and Mute capability. Press `Enter`.
2. On the Attendant Console screen, click **Next** until you see the **Feature Button Assignments** area.
3. In the **Feature Button Assignments** area, perform the following actions:
   - Type `conf-dsp` next to the button that you want the attendant to use for the Conference Display capability.
   - Type `fe-mute` next to the button that you want the attendant to use for the Selective Conference Party Display, Drop, and Mute capability.

4. Press `Enter` to save your changes.

Multiple held calls on a bridge conference

When participants of a conference call put the call on hold and one of the participants resumes the call, the other participants also leave the hold state and resume the in-use state.

Note:

If the on-hold participant presses the Exclusion button and then presses the Resume button, the other participants are dropped out of the call even if they are on a call.

End-user procedures for Conference

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Displaying the participants on a conference call

About this task

Users of a digital telephone and attendants at an attendant console can use the Selective Conference Party Display, Drop, and Mute capability to display information about the participants on a call. When the system displays the information about a participant on a call, a user can drop a participant from the conference call or place a participant on mute.

Procedure

1. Press the conference display feature button to place the station or the console in the conference display mode.
2. Press the conference display feature button repeatedly to scroll through the telephone numbers and names of each participant on the call.

   The telephone number of a participant is always available. The name of a participant might be unavailable.
3. To drop the participant that the system displays, press the **Drop** button.

   This action is useful during a conference call when a user tries to add a participant that does not answer and the call goes to voice mail.
4. To place the participant that the system displays on mute, press the **fe-mute** button.

   The remaining participants on the conference call cannot hear the participant who is on mute. A user or attendant can use the **fe-mute** button to place only one participant on mute, and that participant must be on a trunk call.

This ability to place a conference participant on hold is useful during conference calls when a participant puts the conference call on hold and the system plays music-on-hold to the remaining participants on the conference call.

Caution:

If a user quickly scrolls through the display information repeatedly, the system might take the telephone out of service. If the system takes the telephone out of service, the system resets the telephone, and drops the user from the call.

Considerations for Conference

This section provides information about how the Conference feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Conference under all conditions. The following considerations apply to Conference:

Bridged Appearances

If a station user who is active on a bridged appearance makes a conference or transfer, the user receives enhanced displays based on the Class of Restriction (COR) of the user's station, not the station with the primary extension.

12-party conference

For the 12-party conference feature to work, you must meet the following requirements in addition to configuration in the **Feature-Related System-Parameters** page:

- Avaya Aura® Media Server must exist in any of the connected network regions of the parties that wish to be part of 12-party conference.
- Distributed Communication System (DCS) must be disabled in Feature Administration page of Communication Manager licensing in SMI as well as in SAT.
- If you are using ASAI, then the ASAI link version to AES must be 11 or above.

Trunk-to-Trunk Connections

If you do not allow trunk-to-trunk connections on your system, the system drops all conference participants when:

- A user disconnects.
- All the other participant connect to the conference through trunk lines.

Loss Plan on Conference Calls

The end-to-end total loss for multiparty conference calls that is administered on the Location Parameters screen is not always applied to a specific call. The loss applied to a three-party conference call, for example, is calculated by adding the fixed pairwise loss for each pair of ports to the value for two-party loss shown on the Location Parameters screen. If this total is less than the end-to-end total loss value configured for a three-party conference, calculate the difference, and divide the difference by 2. Add 1 to this figure, and the result is the amount of loss applied to the call.

Interactions for Conference

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

Bridged Call Appearance

A user can use a bridged call appearance to make a conference call. A bridged appearance can bridge onto a conference call if that action does not cause the number of participants on the conference call to exceed six participants. If 12–party conference is enabled, conference call should not exceed 12 participants.

Note:

For 12 parties to participate in a conference, you must enable the **12–party Conferences** field in the Feature-Related System-Parameters screen.

Call Vectoring

A call to a Vector Directory Number (VDN) can be included as a party in a conference call only after vector processing terminates for that call, for example, after a successful route-to command.

Call Waiting

When a user on an analog single-line telephone activates the Call Wait feature, and the user creates a conference call, the Call Wait feature does not function while the user is on the conference call.

Class of Restriction (COR)

If the **Restriction Override** field on the Class of Restriction screen is set to all, the system compares the COR of the participant who controls the conference call with the COR of a new conference participant. The system compares the COR of the participant who controls the conference call with the COR of a new conference participant before the system adds the participant to the conference call. The system does not compare the COR of the new participant with the CORs of the other conference participants.

If the COR of a user, who is controlling the conference call, overrides inward call restrictions, the system compares the COR of the user with the COR of a new conference participant. The system compares the COR of the user who controls the conference call with the COR of a new conference participant before the system adds the new participant to the conference call. The system does not compare the COR of the new participant with the CORs of the other conference participants.

Emergency Access to an Attendant

A user cannot make an Emergency-Access-to-an-Attendant call a participant in conference call.

Trunk-to-Trunk Transfer

The system does not recognize the **Conference** button or the **Transfer** button when a user dials enough digits for the system to route a call, and the system can route the call differently if the user dials more digits. The user must be a user of a multifunction telephone, for example a BRI telephone, a digital telephone, or a hybrid telephone.

If the user wants the system to route the call based on the digits that the user has already dialed, the user must not dial any digits for three seconds, or the user must dial a pound sign (**#**). The system then recognizes the **Conference** button or the **Transfer** button and completes the call.

VDN in a Coverage Path

Calls in an established conference do not cover to a vector directory number (VDN).

Once a call covers to a VDN, a conference cannot be established until the call is delivered to an extension and vector processing ends.

Chapter 66: Data Call Setup

Use the Data Call Setup feature to set up a data call by any of following methods:

- Data-terminal or keyboard dialing
- Telephone dialing
- Hayes AT command dialing
- Permanent-switched connections
- Administered connections
- Automatic-calling unit interface (MPD and HSC)
- Hotline dialing

Detailed description of Data Call Setup

In addition to data-terminal and telephone dialing, the system accepts calls from other devices. For example, you can use a modular-processor data module (MPDM) that is equipped with an automatic-calling unit (ACU) interface module to dial from a host computer.

In addition to the numbers, the pound key (**#**), and the asterisk key (*****) on a telephone, the table on page 593 shows the special characters that a user can dial.

Table 71: Special characters

Character	Short description	Long description
SPACE or minus (-)	and	A space or a minus (-) improves legibility. The server ignores these characters during dialing.
plus (+)	wait	A plus (+) interrupts or suspends dialing until the user receives dial tone.
comma (,)	pause	A comma (,) inserts a 1.5-second delay.
percent (%)	mark	Use a percent (%) to indicate that the digits are for end-to-end signaling when you use a touchtone trunk. Use a percent (%) with a rotary trunk. The percent (%) is not required when you use a touchtone trunk.

Table continues…

Character	Short description	Long description
UNDERLINE or BACKSPACE	-	Use an underline or a backspace to correct characters that you typed on the same line.
at (@)	-	Use an “at” sign (@) to delete the entire line and start again with a new DIAL prompt.

Each line of information that a user dials can contain 42 characters. Note that the system counts the plus (+) and the percent (%) as two characters each.

You administer the asynchronous data module (ADM) as one endpoint of a connection. The server establishes the connection at the scheduled time, and maintains the connection for the specified duration. After the call is accepted, the data set enters into continuous mode for the specified duration. If the server reboots during the connection, or if the connection drops, the server starts the connection again.

The system handles all ISDN basic rate interface (BRI) bearer data-call requests that are presently defined. If the server does not support a capability, the system returns a proper cause value to the terminal.

The system sends a cause code, also called a reason code, to BRI terminals to identify the reason that the system clears a call. The BRI data module converts some cause values to text messages for the system to display. In a passive-bus multipoint configuration, the system supports two BRI endpoints per port, and thus doubles the capacity of the BRI media module. When you change the configuration of a BRI endpoint from point-to-point configuration to a multipoint configuration, the original endpoint does not need to reinitialize. In a multipoint configuration, you can administer only endpoints that support service profile identifier (SPID) initialization.

The table on page 594 shows the call progress messages and the call progress descriptions for digital communication protocol (DCP) and ISDN-BRI modules that the system provides.

Table 72: Call progress messages

Message Code	Module Type	Message Description
DIAL:	DCP	This message is the equivalent of a dial tone. Type the required number or the Feature Access Code (FAC), and then Press `Enter`.
CMD	BRI	This message is the equivalent of a dial tone. Type the required number or the FAC, and then Press `Enter`.
RINGING	DCP, BRI	This message is the equivalent of a ringing tone. The called terminal is ringing.
BUSY	DCP, BRI	This message is the equivalent of a busy tone. The called number is busy or out of service.
ANSWERED	DCP, BRI	The call is answered.
ANSWERED-NOT DATA	DCP	The call is answered, and the system does not detect a modem answer tone.

Table continues…

Message Code	Module Type	Message Description
TRY AGAIN	DCP, BRI	This message is the equivalent of a reorder tone. The system facilities are unavailable.
DENIED	DCP, BRI	This message is the equivalent of an intercept tone. The system cannot place the call as dialed.
ABANDONED	DCP, BRI	The calling user abandoned the call.
NO TONE	DCP, BRI	The system does not detect a tone.
CHECK OPTIONS	DCP, BRI	The data-module options are incompatible.
XX IN QUEUE	DCP, BRI	XX represents the position of the call that is in the queue.
PROCESSING	DCP, BRI	The call is out of the queue. The facility is available.
TIMEOUT	DCP, BRI	The call exceeds the time that is allowed. The system terminates the call.
FORWARDED	DCP, BRI	This message is the equivalent of a redirection-notification signal. The called terminal activates Call Forwarding and receives a call, and the system then forwards the call.
INCOMING CALL	DCP, BRI	This message is the equivalent of ringing.
INVALID ADDRESS	DCP	The user entered a name that is not defined in the Alphanumeric Dialing feature.
WRONG ADDRESS	BRI	The user entered a name that is not defined in the Alphanumeric Dialing feature.
PLEASE ANS-	DCP, BRI	The originating telephone user used the One-Button Transfer to Data capability to transfer the call to a data module.
TRANSFER	DCP	Data Call Return-to-Voice is occurring.
CONFIRMED	DCP, BRI	This message is the equivalent of the confirmation tone. The system either accepts the feature request of the user, or the system sends the call to a local coverage point.
OTHER END	DCP, BRI	The endpoint terminates the call.
DISCONNECTED	DCP, BRI	The system disconnects the call.
WAIT	DCP, BRI	The normal process continues.
WAIT, XX IN QUEUE	DCP	The call is in a local hunt-group queue.

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
- Data-call transfer to voice

Data Call Setup administration

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

- Creating the Data Origination FAC
- Defining a data module
- Specifying the port location
- Assigning the data extension feature button

Related links

Creating the Data Origination FAC on page 597
Defining a data module on page 597
Specifying the modem pool port location on page 605
Assigning the data extension feature button on page 605

Screens for administering Data Call Setup

Table 73: Screens for data-terminal dialing

Screen name	Purpose	Fields
Data Module • PDM/TDM • 7500 • Data Line	Define the data module.	• All • All • All
Modem Pool Group	Specify the port that is associated with the conversion resource on the integrated modem pool circuit pack.	Circuit Pack Assignments

Table 74: Screens for telephone dialing

Screen name	Purpose	Fields
Feature Access Codes	Assign the Feature Access Code (FAC) for data origination.	Data Origination Access Code
Station	Assign the data-ext (Ext:) feature button for data extension.	Any unassigned button field in the area
Data Module • PDM/TDM • Data Line	Define the data module.	• All • All
Modem Pool Group	Specify the port that is associated with the conversion resource on the integrated modem pool circuit pack.	Circuit Pack Assignments

Creating the Data Origination FAC

Procedure

1. Enter `change feature-access-codes`.
2. Click **Next** until you see the **Data Origination Access Code** field.
3. In the **Data Origination Access Code** field, type the FAC for data origination access.
4. Press `Enter` to save your changes.

Defining a data module

Procedure

1. Type `add data-module next`. Press `Enter`.

   The system displays the Data Module screen.

   The system shows two display-only fields in the **Abbreviated Dialing** area. These display only-fields are **Ext** and **Name**. The fields contain the extension number and the name of the users who have associated data extension buttons, and who share this data module.

2. In the **BCC** field, perform one of the following actions:
   - Type `1` if the speed is 56 kbps.
   - Type either `2`, `3` or `4` if the speed is 64 kbps.

     The system compares the speed setting that you assign here with the speed setting in an associated routing pattern. The system compares the two speed settings when calls that attempt to use the data module fail to complete.

     The system displays the **BCC** field if the **ISDN-PRI** field or the **ISDN-PRI Trunks** field on the Optional Features screen is set to y.

3. The **Capabilities** area contains three fields.
   - In the **Busy Out** field, perform one of the following actions:
     - To place the data line circuit (DLC) port in a busy-out state so that calls do not terminate at the data terminal equipment when the DTE control lead to the DLC drops, type `y`. Use this option for DTEs that are members of a hunt group.
     - To keep the DCL .
   - The system displays the **Configuration** field only when the **KYBD Dialing** field is set to y.
     - Type `y` if you want to view and change options from originating or receiving DTEs, such as non intelligent terminals.
     - Type `n` if you do not want view and change options from intelligent devices such as computers.

- In the **KYBD Dialing** field, perform one of the following actions:
  - Type `y` if you want the users to dial calls from a keyboard, and to allow the data module endpoint to transmit and receive text during call origination or call termination.

    If you type `y`, you must also type `n` in the **Low** field in the **Speeds** area of the Data Module screen.
  - Type `n` if you do not want the users to dial calls from a keyboard. If you type `n`, the data module endpoint cannot transmit and receive text during call origination and call termination. If you type `n`, data calls can be answered, but there is no text feedback.

4. The **Circuit Switched Data Attributes** area contains information that is used with 7500 data modules and World Class BRI data modules.

   Note that the fields in the **Circuit Switched Data Attributes** area contain default information. The default information is for modem pooling conversion resource insertion when the endpoint does not support the data query capability, and for when the endpoint does not support the administered connections. The information in the fields has no significance for data modules that provide data query, such as Avaya-supported ISDN-BRI data modules. Use the system default settings that the system provides for Avaya ISDN-BRI data modules or World Class ISDN-BRI data modules.

   - In the **Default Duplex** field, perform one of the following actions:
     - Type `full` for simultaneous, two-way transmission.

       This is duplex mode.
     - Type `half` for only one transmission direction at a time.

       This is half duplex mode.
   - In the **Default Mode** field, perform one of the following actions:
     - Type `sync` for synchronous data mode.
     - Type `async` for asynchronous data mode.
   - In the **Default Speed** field, type the data rate. The valid entries are:
     - 1200
     - 2400
     - 4800
     - 9600
     - 19200
     - 56000 when the **Default Mode** field is set to sync
     - 64000 when the **Default Mode** field is set to sync

5. The system displays the **Connected To** field, when the **Type** field contains either dpm or data-line.

In the **Connected To** field, perform one of the following actions:

- Type `dte` if the Asynchronous Data Unit (ADU) is connected to DTE.
- Type `dte` if the ADU is connected to an information systems network.

6. In the **COR** field, type the number of the class of restriction for this data module.

   Valid entries are 0 through 95.

7. In the **COS** field, type the number of the class of service for this data module.

   Valid entries are 1 through 15.

8. The **Data Module Capabilities** area contains three fields with information for the 7500 data modules and the World Class BRI (WCBRI) data modules.

   - The **Default Data Applications** field identifies the mode that the system uses to originate calls when the calling parameters do not specify the mode. The system also uses the mode to terminate trunk calls that do not have administered connections or for which the bearer capability is unspecified. See the Uniform Dial Plan feature for more information.
   - In the **Default Data Applications** field, perform one of the following actions:
     - Type `M0` to specify mode 0. Use this option for a WCBRI endpoint that the system uses as an administered connection.
     - Type `M1` to specify mode 1.
     - Type `M2_A` to specify mode 2 asynchronous.
     - Type `M2_S` to specify mode 2 synchronous.
     - Type `M3/2` to specify mode 3/2 adaptable.
   - In the **Default ITC** field, perform one of the following actions:
     - Type `restricted` for a WCBRI endpoint that is an administered connection.
     - Type `unrestricted` for a WCBRI endpoint that is not an administered connection.
   - The display-only **MM Complex Voice Ext** field contains the number of the associated telephone in the multimedia complex. The system displays the **MM Complex Voice Ext** field only when the **Multimedia** field is set to y.

     The field is blank until you type the data module extension in the **MM Complex Data Ext** field on the Station screen. When you type the data module extension in the **MM Complex Data Ext** field on the Station screen, the system associates the numbers in the **MM Complex Data Ext and the MM complex Voice Ext** fields as two parts of a one-number complex. The one-number complex is the extension of the telephone.

   The system displays the data module extension in the display-only **Data Extension** field.

9. The system does not display the **ITC** field for voice-only stations or for BRI stations.

   The **ITC** field applies only when the **Comm Type** field on the Trunk Group screen, that the system uses for an outbound call, contains avd or rbavd. The **ITC** field specifies the type of

transmission facilities that an ISDN call uses when a call originates from this data module endpoint.

In the **ITC** field, perform one of the following actions:

- If the data module can send bits at speeds less than or equal to 56 kbps, type `restricted`. If you type `restricted` in the **ITC** field, the system uses a trunk group for which the **COMM Type** field on the Trunk Group screen is set to rbavd or to avd to complete a call from this data module endpoint.

  A restricted transmission facility enforces ones density digital transmission. Ones density digital transmission is a sequence of eight digital zeroes that the firmware on the DS1 port board converts to a sequence of seven zeroes and a digital 1.

- If the data module can send bits at a speed no greater than 64 kbps, type `restricted`. If you type `unrestricted` in the **ITC** field, the system uses a trunk group for which the **COMM Type** field on the Trunk Group screen is set to avd to complete a call from this data module endpoint. The value avd in the **Comm Type** field indicates that the trunk group provides both restricted and unrestricted transmission facilities.

  An unrestricted transmission facility does not enforce ones density digital transmission. The DS1 port board firmware does not convert the digital information.

10. In the **List1** field in the **ABBREVIATED DIALING** area, perform one of the following actions:
    - Leave the field blank if you do not want the data module to have an abbreviated dialing list.
    - Type `e` if you want the data module to have an enhanced abbreviated dialing list.
    - Type `g` if you want the data module to have a group list. If you type `g`, the system displays a field to the right of the **List1** field. If you type `g` in the **List1** field, you must also type a group list number in the field that the system displays.
    - Type `p` if you want the data module to have a personal list. If you type `p`, the system displays a field to the right of the **List1** field. If you type `p` in the **List1** field, you must type a personal list number in the field that the system displays.
    - Type `s` if you want the data module to have a system abbreviated dialing list.
11. In the **Name** field, perform one of the following actions:
    - Type the name of the user who is associated with the data module.
    - Leave the field blank.
12. The **OPTIONS** area contains six fields.
    - The system displays the **Answer Text** field only if the **KBDY Dialing** field is set to y.

      The **Answer Text** field applies to the following call messages:

      - Incoming
      - Answered

- Disconnected
- Disconnected other end

In the **Answer Text** field, perform one of the following actions:

- Type `y` to enable text feedback to the DTE when a user answers a call or the system disconnects a call. The text feedback includes both DLC-generated text and system-generated text.
- Type `n` to disable text feedback to the DTE when a user answers a call or the system disconnects a call, and when the DTE that answers a call is a computer or an intelligent device. The system still generates the text, but the DLC does not support delivery of the text to the DTE.

- The system displays the **Connected Indication** field only if the **KBDY Dialing** field is set to y. If the **Connected Indication** field is set to n, DLC provides the connection indication when the DLC activates the Electronics Industries Association (EIA) 232C control lead.

  In the **Connected Indication** field, perform one of the following actions:

  - Type `y` if you want the system to generate a connected message to the DTE when the system establishes a connection.
  - Type `n` if you do not want the system to generate a connected message to the DTE when the system establishes a connection.

- The system displays the **Dial Echoing** field only if the **KBDY Dialing** field is set to y.

  In the **Dial Echoing** field, perform one of the following actions:

  - Type `y` if you want the system to echo characters back to the DTE.
  - Type `n` if you do not want the system to echo characters back to the DTE and when an intelligent device provides keyboard dialing.

- The system displays the **Disconnect Sequence** field only if the **KBDY Dialing** field is set to y.

  In the **Disconnect Sequence** field, perform one of the following actions:

  - Type `long-break` if you want a break that is greater than 2 seconds.
  - Type `two-breaks` if you want a break that is less than 1 second.

- The system displays the **Parity** field only if the **KBDY Dialing** field is set to y. The DLC generates the parities when the DLC sends call setup text to the DTE. The DLC does not check the parity when the DLC receives dial characters. Select the parity that matches the DTE that connects to the data module.

  In the **Parity** field, type one of the following types of parity:

  - even
  - odd

- mark
- space

- The **Permit Mismatch** field contains information that is used by an EIA interface to operate at a rate that differs from the rate that is agreed upon during the data module handshake. The rate that is agreed upon during the data module handshake is always the highest compatible rate among the speeds that each data module reports.

  The information in the **Permit Mismatch** field eliminates the need to change the DTE or DLC speed whenever someone, or something, places a call to or from endpoints that operate at a different speed.

  When the **Permit Mismatch** field is set to y, the DLC reports the highest optional speed and all the lower speeds, or the previously selected autoadjust speed, during the handshake process.

  - Type `y` If you want the DLC to operate at the highest selected speed, which is a higher rate than the far-end data module.
  - Type `n` if you do not want DLC to operate at the highest selected speed.

13. In the **Port** field, type the appropriate values from the table on page 602.

Table 75: Port field values

Characters	Description	Value
1-3	Gateway number	G4xx Media Gateway Number
4	Gateway	V
5	Slot number	1 through 8
6-7	Circuit number	Port number on media module
x	Administration without Hardware	If the **Secondary data module?** field, is set to n, you can type `x` in the **Port** field. A **Port** field set to x indicates that no hardware is associated with the port assignment.

14. The **SPEEDS** area contains information about the operating speeds of the data module.
    - In the **Low** field, perform one of the following actions:
      - Type `y` if you want the data line circuit to operate at a speed of 0 to 1800 bps.
      - Type `n` if the **KYBD Dialing** field in the **CAPABILITIES** area is set to y.
    - In the **300**, **1200**, **2400**, **4800**, **9600**, and **19200** fields, perform one of the following actions:
      - Type `y` if you want the DLC to operate at the speed.

        You can choose any of the speeds for the DLC. The DLC matches the speed for the duration of the call.

        If you select multiple speeds, you must also set the **Autoadjust** field to n and select at least three speeds. The speed of the DTE must be the highest speed that you

select. The DTE must have the highest speed because the system delivers feedback to the DTE at the highest selected speed.

- Type `n` if you do not want the DLC to operate at the speed.

- The system displays the **Autoadjust** field when the **KYBD Dialing** field in the **CAPABILITIES** area is set to y. The **Autoadjust** field applies only to calls that a user originates from a keyboard.

  In the **Autoadjust** field, perform one of the following actions:

  - Type `y` if you want the DLC port to automatically adjust to the operating speed and the parity of the DTE to which the DLC port connects.
  - Type `n` if you do not want the DLC port to automatically adjust to the operating speed and the parity of the DTE to which the DLC port connects.

15. In the **Special Dialing Option** field, perform one of the following actions:
    - Leave the field blank if you do not want the data module to have special dialing.
    - Type `hot-line` if you want the data module to have hot-line dialing. If you type `hot-line`, the system displays the **Abbreviated Dialing Dial Code (from above list):** field. Type the abbreviated dial code in the **Abbreviated Dialing Dial Code (from above list):** field. Valid entries are 0 through 999.
    - Type `default` if you want the data module to have default dialing. If you type `default`, the system displays the **Abbreviated Dialing Dial Code (from above list):** field. Type the abbreviated dial code in the **Abbreviated Dialing Dial Code (from above list):** field. Valid entries are 0 through 999.
16. In the **TN** field, type the tenant partition number of the data module.

    Valid entries are 1 through 100.
17. In the **Type** field, perform one of the following actions:
    - To assign a 7500 data module, type `7500`.

      The 7500 data module supports:

      - Automatic TEI
      - B-channel, maintenance and management messaging
      - Service Profile Identifier (SPID) initialization capabilities.

        BRI voice endpoints, BRI data endpoint, or both BRI voice and BRI data endpoints are assigned to either the ISDN-BRI - 4-wire S/T-NT Interface circuit pack or the ISDN-BRI - 2-wire U circuit pack. Each circuit pack can support up to 12 ports.

        You can administer more than one ISDN endpoint, either a voice endpoint or a data endpoint, on one port. You can administer more than one ISDN endpoint, because BRI provides a multipoint capability.

        For BRI, telephones that have SPID initialization capabilities use multipoint administration. Multipoint administration is allowed only if no endpoint that is administered on the same port is a fixed tie endpoint, and no station on the same

port has B-channel data capability. The system restricts multipoint administration to two endpoints per port.

- Type `data-line` to assign a data line data module.

  Use the Data Line Data Module (DLDM) screen to assign ports on the Data Line (DLC) circuit pack for EIA 232C devices to connect to the system. The DLC, with a companion ADU, provides a less expensive data interface to the system than other asynchronous DCP data modules.

  The DLC supports asynchronous transmissions at speeds of Low and 300, 1200, 2400, 4800, 9600, and 19200 bps over 2-pair (full-duplex) lines. These lines can have different lengths, depending on the transmission speed and the wire gauge.

  The DLC has eight ports. The connection from the port to the EIA device is direct, which means that no multiplexing is involved. A single port of the DLC is equivalent in functionality to a data module and a digital line port. The system displays DLC as a data module to the DTE and as a digital line port to the server that runs Communication Manager.

  The DLC connects the following EIA 232C equipment to the system:

  - Printers
  - Non intelligent data terminals
  - Intelligent terminals, personal computers (PCs)
  - Host computers
  - Information Systems Network (ISN), RS-232C local area networks (LANs), or other data switches

- Type `pdm` to assigns a DCE interface for processor data modules or trunk data modules.

  Use these screens assign Modular Processor Data Modules (MPDMs) and Modular Trunk Data Modules (MTDMs). Use one screen to assign MPDMs (700D), 7400B, 7400D or 8400B Data Module. Use another screen for MTDMs (700B, 700C, 700E, 7400A). You must complete one screen for each MPDM, 7400B, 7400D, 8400B or MTDM.

  The MPDM, 7400B, or 8400B Data Module provides a Data Communications Equipment (DCE) interface. Use the interface for a connection to equipment such as a data terminal, call detail recording (CDR) output device, on-premises administration terminal, Message Server, Property Management System (PMS), Communication Manager Messaging, and host computers. The MPDM, 7400B, or 8400B Data Module also provides a Digital Communications Protocol (DCP) interface to the digital switch.

  Note that DCE is the equipment on the network side of a communications link that provides all the functions that are required to make the binary serial data from the source or transmitter compatible with the communications channel.

  The MTDM provides an EIA DTE interface for connection to off-premises private line trunk facilities, or a switched telecommunications network and a DCP interface for connection to the digital switch. Note that DTE is the equipment that comprises the

endpoints in a connection over a data circuit. For example, in a connection between a data terminal and a host computer, the terminal, the host, and their associated modems or data modules make up the DTE. The MTDM or the 7400A Data Module can also serve as part of a conversion resource for combined modem pooling.

18. Press `Enter` to save your changes.

Specifying the modem pool port location

Procedure

1. Type `change modem-pool num` *n*, where *n* is the modem pool that you want to change. Press `Enter`.

   The system displays the Modem Pool Group screen.

2. In the **Circuit Pack Location** field, type the 7-character port number that is associated with the conversion resource on the integrated modem pool circuit pack.

   Information in the **Circuit Pack Location** field is optional for integrated conversion resources only.

3. Press `Enter` to save your changes.

Assigning the data extension feature button

Procedure

1. Type `change station` *n*, where *n* is the telephone number of the user that you want to change. Press `Enter`.
2. On the Station screen, click **Next** until you see the **Button Assignments** area.
3. Type `data-ext` after any available button number.

   When you type `data-ext` in a field, the system displays an **Ext:** field.

4. Type the extension of the data module in the **Ext:** field.
5. Press `Enter` to save your changes.

End-user procedures for Data Call Setup

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Setting up and disconnecting data calls from a DCP data terminal

Procedure

1. At the Dial: prompt, type the data number.

The system displays the RINGING message.

If the call is in a queue, the system displays the WAIT, XX IN QUEUE message. The system displays the position of the call in the queue, represented by XX, as the system moves the call through the queue.

2. Press `Break` to originate or disconnect a call.
3. If the terminal does not generate a 2-second continuous break signal, press the **originate/disconnect** button on the data module.
4. At the DIAL: prompt, type the digits.

Setting up data calls from a DCP telephone

About this task

When a data terminal is unavailable, you can originate and control data calls from a DCP telephone. Use any unrestricted telephone to set up the call, and then transfer the call to a data module endpoint.

Use a button on a multiappearance telephone data-extensions to make the data call. Assign any administrable feature button as a data-extension button. The data-extension button provides one-touch access to a data module.

Use any of the following options, either alone or in combination, to make a data call from a voice terminal.

Procedure

1. One-Button Transfer to Data

   Press the **data-extension** button after the endpoint answers, to transfer a call to the associated data module.

2. Return-to-Voice

   Press the **data-extension** button that is associated with a busy data module to change a connection from a data connection to a voice connection. If you hang up, the system disconnects the call. If the system returns the data call to the telephone, the system either continues the call in voice mode, or the system transfers the data call to another endpoint.

3. Data Call Preindication

   Press the **data-extension** button to reserve the associated data module before you dial a data endpoint. The system reserves the data module for the call and reserves a conversion resource for the call, if the call needs a conversion resource.

   Use the Data Call Preindication option before you use one-button transfer to data, for data calls that use toll-network facilities. Data Call Preindication is in effect until you press the associated **data-extension** button again for a one-button transfer. There is no timeout.

Setting up and disconnecting data calls from an ISDN-BRI data terminal

Procedure

1. Press `Enter` a few times until the system displays the CMD: prompt.
2. If the system does not display the CMD: prompt:
   a. Press `Break`, `A`, and `T` at the same time.
   b. Press `Enter`.
   c. Type three plus signs (`+++`).

      The system displays the CMD: prompt.
   d. Type `end`.
   e. Press `Enter`.

Setting up data calls from an ISDN-BRI telephone

Procedure

1. Press the data button on the telephone.
2. Type the number on the dial pad.
3. Press the data button again.

   The following data functions are unavailable on ISDN-BRI voice terminals:

   - One-button transfer to data
   - Return-to-voice
   - Data call preindication
   - Voice call transfer to data, and data call transfer to voice

Considerations for Data Call Setup

This section provides information about how the Data Call Setup feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Data Call Setup under all conditions. The following considerations apply to Data Call Setup:

- ISDN basic rate interface (BRI) has a voice-to-data restriction. A telephone cannot call a data terminal, and a data terminal cannot call a telephone
- BRI telephones cannot have data-extension buttons. Digital Communications protocol (DCP) sets have data-extension buttons. However, DCP sets cannot have data-extension buttons for BRI.

- When a telephone user uses a modem to place a data call, the user dials the data-origination access code that is assigned in the system before the user dials the endpoint.
- The system does not limit the number of assigned data-extension buttons per telephone. Assign telephone buttons that access the data module.
- Telephone dialing is unavailable in ISDN-BRI applications because ISDN-BRI terminals supports neither voice-call transfer to data, nor data-call transfer to voice.

Interactions for Data Call Setup

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

Abbreviated Dialing

You can use only 22 of the 24 digits in an abbreviated-dialing number when you dial at a keyboard. The remaining two digits must contain the wait indicator for tone detection.

Alphanumerical Dialing

When a data-terminal user uses the Alphanumeric Dialing feature to place a call, the user enters an alphanumeric name.

Call Coverage

You cannot assign a coverage path to a hunt group that consists of data endpoints.

Call Detail Recording (CDR)

CDR records the use of modem pools on trunk calls.

Call Forwarding All Calls

The system uses the Call Forwarding All Calls capability to redirect data calls to a user-designated extension. The attendant or a forwarding party dials a Feature Access Code (FAC) to activate the Call Forwarding All Calls capability.

A user can use data-terminal dialing to activate Call Forwarding All Calls for calls to a data module. If the forwarded-to endpoint is an analog endpoint, and the caller is a digital endpoint, the system activates modem pooling automatically.

Data Hotline

Data Hotline is a security feature. The server terminates calls to a preadministered hotline. The system discards any address string and routes the call as if the users entered the hotline-destination address. This Data Hotline feature does not affect incoming calls. You cannot use the Data Hotline feature and the Default Dialing feature at the same time.

Default Dialing

If the Default Dialing feature is active, a data-terminal user can Press `Enter` to call a preadministered destination. The data-terminal user enters a complete address to call other destinations.

Digit Dialing

The system provides basic digit dialing through an asynchronous data module (ADM) or a 7500B data module. The user can enter digits from 0 to 9, an asterisk (*), and a pound sign (#) from a 7500 series telephone keypad or from an Electronics Industries Association (EIA)terminal interface.

Internal Automatic Answer

Data calls are ineligible for Internal Automatic Answer.

Modem Pooling

Modem Pooling is available on data calls. The system automatically inserts a modem if the data call needs a modem. You can use the Data Call Preindication option or the Data Origination option to indicate the need for a modem.

Uniform Call Distribution (UCD)

UCD provides a group of data modules, or analog modems, for answering calls to a connected facility. A computer port is an example of a connected facility.

World-Class Tone Detection

The system supports multiline data-terminal dialing, if you set the **tone-detection options** field on the Feature-Related System-Parameters screen to precise.

The message that Data Call Setup sends to users depends on the tone-detection option that you administer.

Chapter 67: Default Dialing

Use the Default Dialing feature to provide data-terminal users who often dial the same number a very simple method to dial that number. Normal data-terminal dialing and the alphanumeric dialing features are unaffected.

Detailed description of Default Dialing

Data terminal users use the computer keyboard to dial. With Default Dialing, a data-terminal user can place a data call to a pre-administered destination by doing either of the following:

- Pressing `Enter` at the DIAL: prompt (for data terminals using DCP 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).

- Typing `d` and pressing `Enter` at the CMD: prompt. For data terminals that use ISDN-BRI data modules.

  To place calls to other destinations, the user calls types `d`, a space, the complete address, and press `Enter` after the CMD: prompt.

Note:

DU-type hunt groups that connect the system to a terminal server on a host computer have hunt-group extensions set to no keyboard dialing.

Default Dialing administration

This section describes the screens that you use to administer the Default Dialing feature.

Screens for administering Default Dialing

Screen name	Purpose	Fields
Data Module	Set the default dialing options.	• Special Dialing Option • Abbreviated Dialing List • AD Dial Code

Chapter 68: Delayed Caller ID Alerting for Name Display Update

Use this feature to administer the delayed caller ID information sent to the analog telephone.

Detailed description of Delayed Caller ID Alerting for Name Display Update

For analog telephones, the caller ID information (caller's number and name) is sent to the telephone as a burst between the first and second rings. When a call is received over an ISDN trunk in North America, the caller information can be delivered either in the SETUP message or in a subsequent FACILITY message.

The display for IP and digital telephones can be updated with the caller information, based on the **US NI Delayed Calling Name Update** field on ISDN Trunk Group screen.

For analog caller ID telephones, the Delayed Caller ID Alerting for Name Display Update feature enables the following:

- Communication Manager waits for the FACILITY message before delivering an incoming call to the called user.
- Administer the time to wait for the FACILITY message which includes the caller information.

If no FACILITY message is received before the timer expires, the called analog telephone rings without displaying the caller ID information.

Delayed Caller ID Alerting for Name Display Update administration

The following steps are the part of the administration process for the Delayed Caller ID Alerting for Name Display Update feature:

- Enabling Delayed Caller ID Alerting for Name Display Update
- Setting delay of caller information for analog telephones

Screens for administering Delayed Caller ID Alerting for Name Display Update

Screen name	Purpose	Fields
Trunk Group	Enable the Delayed Caller ID Alerting for Name Display Update feature.	US NI Delayed Calling Name Update
Feature-Related System Parameters	Set the timer to delay the display of caller information for analog telephones.	Delay for USNI Calling Name for Analog Caller ID Phones (seconds)

Enabling Delayed Caller ID Alerting for Name Display Update

Procedure

1. Type `change trunk-group n`, where *n* is the number of the trunk group. Press `Enter`.
2. Ensure that the **Group Type** field is set to isdn.
3. Click **Next** till you see the **US NI Delayed Calling Name Update** field.
4. Set the **US NI Delayed Calling Name Update** field to `y`.
5. Press `Enter` to save your changes.

Setting Delay of Caller Information for Analog Telephone

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. Click **Next** till you see the **Delay for USNI Calling Name for Analog Caller ID Phones (seconds)** field.
3. In the **Delay for USNI Calling Name for Analog Caller ID Phones (seconds)** field, set the number of seconds.
4. Press `Enter` to save your changes.

Interactions for Delayed Caller ID Alerting for Name Display Update

This section provides information about how the Delayed Caller ID Alerting for Name Display Update feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Delayed Caller ID Alerting for Name Display Update in any feature configuration.

Groups

The incoming call is not delayed, if the analog telephone is a member of a group. For example, hunt group, TEG, and coverage answer group. The display on the analog telephone includes the caller's number.

Bridging

Communication Manager delays ringing a call to an analog telephone, even if it has an analog bridged appearance on a digital telephone.

X-Ports

The incoming call is delayed even if the analog telephone is an X-port with bridged appearances on digital telephones.

Call Forwarding All

If calls to a digital telephone are forwarded to an analog Caller ID telephone using Call Forward All, the call to the analog telephone is not delayed since Communication Manager only delays alerting for the initial incoming call. However, the caller information may still display on the analog Caller ID telephone, if the caller information is received from the ISDN network before the analog telephone rings.

If calls to an analog Caller ID telephone are forwarded to another analog Caller ID telephone using Call Forward All, the call to the first analog telephone is not delayed since the call is immediately redirected to the second analog telephone. However, the caller information may still display on the second analog Caller ID telephone, if the caller information is received from the ISDN network before the analog telephone rings.

Call Forwarding Don't Answer

If calls to an analog Caller ID telephone are forwarded to another analog Caller ID telephone using Call Forwarding Don't Answer, the call to the first analog telephone is delayed. However, the forwarded call to the second analog Caller ID telephone is not delayed since Communication Manager only delays alerting for the initial incoming call.

If calls to a digital telephone are forwarded to an analog Caller ID telephone using Call Forwarding Don't Answer, the call to the analog telephone is not delayed since Communication Manager only delays alerting for the initial incoming call. However, the caller information can still display at the analog Caller ID telephone, if the caller information is received from the ISDN network before the analog telephone rings

Out-of-Service

The incoming call is delayed even if the analog telephone is out of service with bridged appearances on digital telephones.

Caller ID Call Waiting

The caller name/number displays for the delayed call that rings as a Call Waiting call if the Call Waiting Caller ID is administered for the endpoint.

Chapter 69: Delayed drop on receiving DISC

Enhanced support for SIP Contact Centers on failed outgoing ISDN calls

When a Voice Portal agent makes a call to a PSTN user and the call is routed over an ISDN trunk and if the PSTN disconnects the call before the called party can answer, the PSTN might send an indication to Communication Manager to delay the call drop until the PSTN completes playing an announcement or tone to the caller. The delay in call drop keeps the Voice Portal agent busy while the announcement or tone is being played to the caller, even though the agent cannot actually hear the announcement or tone.

With Communication Manager Release 6.3.6 onwards, you can use the **Interworking of ISDN Clearing with In-Band Tones** field on the **SIP Trunk** form to communicate the reason of the call drop to the caller.

After knowing that the called party will not answer the call, the caller or the Voice Portal agent can decide whether to end the call immediately or wait for the announcement or tone to complete.

If you set the **Interworking of ISDN Clearing with In-Band Tones** field to **drop-with-sip-error**, Communication Manager sends the reason for the call being dropped by the called party.

If you set the **Interworking of ISDN Clearing with In-Band Tones** field to **keep-channel-active**, the call drop is delayed till the complete announcement or tone is being played to the caller.

Chapter 70: Demand Print

Use the Demand Print feature to print undelivered messages.

Detailed description of Demand Print

With Demand Print, a user can dial a Feature Access Code (FAC) or press a button to print undelivered messages.

Demand Print administration

This section describes the screens that you use to administer the Demand Print feature.

Screens for administering Demand Print

Screen name	Purpose	Fields
Feature Access Code (FAC)	Specify the FAC for Demand Print.	Print Messages Access Codes
Station (multiappearance)	Assign a print-messages feature button for a user.	Any available field in the **Feature Button Assignments** area
	Assign a Station Security Code (SSC) for a user.	Security Code

Chapter 71: Dial Access to Attendant

Use the Dial Access to Attendant feature to dial an attendant access code and reach an attendant.

Detailed description of Dial Access to Attendant

With the Dial Access to Attendant feature, telephone users in your system can use an attendant access code to reach an attendant. Attendants can then extend the call to a trunk, or to another telephone.

Dial Access to Attendant administration

The following step is part of the administration process for the Dial Access to Attendant feature:

- Changing the attendant access code

Related links

Changing the attendant access code on page 617

Screens for administering Dial Access to Attendant

Screen name	Purpose	Fields
Dial Plan Analysis Table	Change the attendant access code from the default setting of 0.	• Dialed String • Total Length

Changing the attendant access code

About this task

You can administer the length of the attendant access code. The attendant access code can be a 1-digit or 2-digit number. The default attendant access code is 0.

Note:

If you have multiple locations, you can also change the attendant access code from the Locations screen. For more information, see the Multi-Location Dial Plan feature.

Procedure

1. Enter `change dialplan analysis`.
2. To assign a digit other than 0, find attd in the **Call Type** column.

   In that row:

   - Change the number in the **Dialed String** column to a unique 1-digit or a 2-digit number.
   - If you changed the number in the **Dialed String** column to a 2-digit number, change the number in the **Total Length** column to `2`.
3. Select **Enter** to save your changes.

   You can also enter a fac or dac entry on the Dial Plan Analysis Table screen to administer the attendant access code. You then enter the actual access code on the Feature Access Codes screen. You can administer location-specific attendant access codes on the Locations screen.

   For more information, see the Dial Plan feature and the Feature Access Code feature.

Interactions for Dial Access to Attendant

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

Class of Restriction

If the Class of Restriction (COR) of a telephone restricts a user from originating calls, the user cannot call the attendant.

Conference

If a telephone user dials the attendant access code, the attendant cannot add that user to an existing conference call.

Chapter 72: Dial Plan

Use the Dial Plan feature to interpret the digits that a user dials. The system needs this information to properly route the call. The Dial Plan feature supports intraserver dialing for extensions that are co-located with the server, and for extensions that are spread across several locations.

Detailed description of Dial Plan

Use the Dial Plan feature to provide the information that the software uses to interpret the digits that a user dials. The software needs this information to properly route the call. The Dial Plan feature supports intraserver dialing for extensions that are co-located with the server, and for extensions that are spread across several locations.

If you need a dial plan that supports interserver dialing, see the Uniform Dial Plan feature.

Dial Plan enhancements for Communication Manager

Beginning with Communication Manager Release 4.0, the Dial Plan feature has been expanded to accommodate maximum extension lengths of 16 digits, and allow 18-digit extension dialing using the Uniform Dial Plan (see the Uniform Dial Plan feature). This expansion to 16 digits permits Communication Manager to support the Open Numbering plan that is offered by the Tenovis I55, as well as by other vendors.

This expansion to 16 digits also involves full support for short/long number dialing, flexible punctuation formats, and flexible extension lengths in call appearance and button labels. For US customers, the Dial Plan Expansion feature improves the Dial Plan. Communication Manager can fit more easily into European networks with numbering plans of 8 or more digits (notably those that use Open Numbering).

Punctuation of long numbers, introduced in Communication Manager 1.3 for 6-digit and 7-digit extensions, is still supported for the new longer extensions. Communication Manager 4.0 or later extends this capability to administration forms as well. With punctuation, customers can more easily read extensions of eight or more digits.

The Multi-location Dial Plan feature that was introduced in Communication Manager 2.0 has been extended for Communication Manager 4.0 or later. This means that a customer can let their users dial short numbers within a location. For example, a user can dial 66180 instead of having to dial the full extension 1-908-456-6180. Beginning with Communication Manager 4.0, customers have the option to display the short number on station displays rather than the full extension.

Note:

The Dial Plan Expansion feature affects the information that is displayed on a display telephone. The display information changes based on the type of telephone. However, when extensions longer than 8 characters displays on a telephone, some display strings had to be modified for everything to fit. For example, on a normal station-to-station call, if the punctuated extension is longer than 8 digits, the last three letters of the 27-character name are truncated.

The expanded dial plan is intended to support the “flatten and consolidate” architecture that Avaya is offering to customers with large DCS and QSIG networks. It simplifies administration, since only a few Communication Manager servers need to be managed rather than dozens or even hundreds of small switches. Communication Manager Release 4.0 or later makes this consolidation easier by letting users keep seeing and dialing their shorter extensions even as their actual extensions grow larger.

Note:

Starting with Communication Manager Release 5.0, you can also use the Per-Location Dial Plan feature for different branches to have different short extensions, so that the extensions do not conflict across branches.

The Dial Plan Expansion feature is implemented on all Linux-based server platforms.

Some of the screens that are modified to accommodate the longer extensions, or have new fields added to them, are:

- Dial Plan Analysis screen
- Dial Plan Parameters screen
- Location Parameters screen
- Station screen
- Uniform Dial Plan Table screen

For more detailed information, see the *Avaya Aura® Communication Manager Screen Reference*.

Dial Plan is enhanced in Communication Manager 6.0 and later to introduce dial prefixes to be dialed before an extension. These dial prefixes are not part of the extension. This enhancement provides a way to avoid dial plan conflicts between long, unique extensions and short numbers used for dialing within a branch or a location. Using dial prefix, you can consolidate E.164 extensions in one digit block, which frees up other leading digits for short intra-branch dialing.

A sample scenario where the dial prefix enhancement is helpful:

- Single Communication Manager server with gateways in two or more countries.
- Extensions that match E.164 public numbers.
- Short dialing within locations and branches.
- Countries involved have long E.164 numbers.

Avaya recommends that you put extensions into a block of numbers with a single leading digit or group of digits. This keeps the other leading digits available for short intra-branch dialing. In some

branches, public E.164 numbers can be 16 digits long, which means there is no room for an extra leading digit. A dial prefix gives you a way to work around this limitation.

For information on how to set up dial prefixes, see Setting up dial prefixes.

Dial plan information

The system supports several types of calls. You must define dial plan information for each type of call.

- Attendant
- Automatic alternate routing (AAR)
- Automatic Route Selection (ARS)
- Dial access codes (DACs), which includes Feature Access Codes (FACs) and trunk access codes (TACs)
- Enbloc extensions (enb-ext)
- Extensions
- FACs only
- Prefixed extensions

You must also define dial plan information for all calls, regardless of the type of call. You also can define information that controls the appearance of extensions up to 16 digits that the system displays for users and attendants.

If the users on your server are at several physical locations, you need to define additional dial plan information about the locations.

Dial Plan Analysis Table

The Dial Plan Analysis Table is the guide that the software uses to translate the digits dialed by users. This screen enables you to determine the beginning digits and total length for each type of call that Communication Manager needs to interpret.

Use the Dial Plan Analysis Table screen to define the dial plan for your system.

- Call Type - Indicates what the system does when a user dials the digit or digits indicated in the **Dialed String** column. The Dial Plan Analysis Table screen contains the following call types:
  - Attendant (attd) - Defines how users call an attendant. Attendant access numbers can be any number from 0 to 9 and contain 1 or 2 digits.
  - Dial access code (dac) - You can use trunk access codes (TAC) and Feature Access Codes (FACs) in the same range. For example, you could define the group 100 -199, which would allow both FAC and TAC in that range. Dial access codes can start with any number from 1 to 9, * and #, and contain up to 4 digits.

Note:

You cannot enter a range specifically for trunk access codes on the Dial Plan Analysis Table screen. However, with the Trunk Group screen you can assign a TAC to a trunk group. The TAC you enter on the Trunk Group screen must match the format you have administered for a DAC on the Dial Plan Analysis Table screen.

- Enbloc extensions (enb-ext) - Defines a block of extensions that must be dialed using a prefix when the caller dials from a keypad. These extensions can be dialed without a prefix if the caller dials enbloc, for example, from a station call log.

Important:

To avoid dial plan conflicts, Avaya recommends you to put all extensions under the same first digit or group of digits, leaving the other leading digits free for short dialing within a branch.

- Extensions (ext) - Defines extension ranges that can be used on your system.
- Feature access codes (fac) - FAC can be any number from 1 to 9 and contain up to 4 digits. You can use * or #, but only as a first digit.
- Uniform Dial Plan (udp) - The udp call type works identically with the ext call type, with this exception:
  - If dialed digits match the call type of udp, Communication Manager automatically checks the UDP Table first to see if there is a match, regardless of the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen. If there is no match, Communication Manager then checks the local server.
  - If dialed digits match the call type of ext, Communication Manager checks the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen.
    - If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is udp-table-first, Communication Manager checks the UDP Table first to see if there is a match. If there is no match, Communication Manager then checks the local server.
    - If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is local-extensions-first, Communication Manager checks the local server first to see if there is a match. If there is no match, Communication Manager then checks the UDP Table.

  With the udp call type, Communication Manager can recognize strings of 14 and 15 digits, which are shorter than the maximum extension length of 18 digits. However, the udp call type can be used with any length in case this provides a useful new capability to customers.

Note:

If you are administering a Per-Location Dial Plan, you must use the Uniform Dial Plan feature.

- Total Length - Indicates how long the dialed string will be for each type of call.

Dial Plan Parameters

The Dial Plan Parameters screen works with the Dial Plan Analysis Table to fully define the dial plan of your system. On the Dial Plan Parameters screen, you can set system-wide parameters for your dial plan. The Dial Plan Parameters screen also controls the appearance of 8-digit and 13-digit extensions on station displays. You can select a system-wide format to display all 8-digit extensions, and a format to display all 13-digit extensions.

For more information on fields in the Dial Plan Parameters screen, see *Administering Avaya Aura® Communication Manager*.

Multi-location Dial Plan overview

When a customer migrates from a multiple independent node network to a single distributed server whose gateways 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 that were provided in a multiple independent node network, but appear to be unavailable when customers migrate to a single distributed server.

Multi-location dial plan short dialing

Users in small locations might not like dialing 7 digits to reach the person across the hall. Also, customers want to set up their system, like retail stores, so that the same extension is used for the same department in each store, even if each store uses a gateway connected to a central Communication Manager server.

This is solved using a new special entry on the UDP screen that tells the system to “transfer” the leading digits of the calling party’s telephone number to the dialed number. For example, if extension 852-5581 dials 23529, the leading 85 is prepended and 852-3529 is called. However, the station displays all show the long number (852-xxxx), not the shorter dialed number (2xxxx). This is the default behavior. Starting from Communication Manager Release 4.0, you can use the Intra-Location formats on the Dial Plan Parameters screen to display the shorter, dialed numbers.

Multi-location dial plan location prefix

The system adds the prefix assigned to the location of the user to the digits that the user dials. The server then analyzes the combined string and routes the call. The system uses several sources for the location information. For information on location per station, see the Detailed description of Administer location per station section.

Related links

Detailed description of Administer location per station on page 103

Multi-location dial plan location prefix example

For example, in a department store with many locations, each location might have had its own switch with a multiple independent node network. The same extension could be used to represent

a unique department in all stores (extension 4567 might be the luggage department). If the customer migrates to a single distributed server, a user could no longer dial 4567 to get the luggage department in their store. The user would have to dial the complete extension to connect to the proper department.

Instead of dialing a complete extension, users can use the multi-location dial plan feature and dial a shorter version of the extension. For example, a customer can continue to dial 4567 instead of having to dial 123-4567.

Communication Manager takes the location prefix and adds those digits to the front of the dialed number. The switch then analyzes the entire dialed string and routes the call based on the administration on the Dial Plan Parameters screen.

Other options for Dial Plan

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

Dial Plan administration

The following tasks are part of the administration process for the Dial Plan feature:

1. Defining a dial plan
2. Adding extension ranges
3. Defining a multi-location dial plan
4. Setting up dial prefixes

Related links

Defining a dial plan on page 625
Adding extension ranges to a dial plan on page 626
Defining a multi-location dial plan on page 626
Setting up dial prefixes on page 626

Screens for administering Dial Plan

Screen name	Purpose	Fields
Dial Plan Analysis Table	Specify the dial plan information for each type of call.	All

Table continues…

Screen name	Purpose	Fields
Dial Plan Parameters	Specify system-wide parameters for a dial plan.	All
Locations	If a network consists of multiple locations, provide information about those locations.	• ARS FAC • ARS Prefix 1 Required for 10-Digit NANP Calls? • Attd FAC • Loc Number • Loc. Parms. • Name • NPA • Prefix
Optional Features	If a network consists of multiple locations, ensure that the system is enabled to support those locations.	Multiple Locations

Defining a dial plan

Procedure

1. Type `change dialplan analysis`.
2. Press `Enter`.

   The system displays the Dial Plan Analysis Table screen.
3. Move the cursor to an empty row.
4. In the **Dialed String** field, type the initial digits that a user might dial.

   The dialed string contains the digits that Communication Manager analyzes to determine how to process the call.
5. In the **Total Length** field, type the total number of digits that a user must dial for this dialed string.

   Note:

   To administer a per-Location dial plan, use the Uniform Dial Plan feature.
6. In the **Call Type** field, type the name of the call type for this dialed string.

   Note:

   The **Percent Full** field displays the percentage of the system memory resources allocated for the dial plan that are currently in use.
7. Save the changes.

Adding extension ranges to a dial plan

About this task

Before you assign a telephone to an extension, ensure that the extension belongs to a range that is defined in the dial plan. The following sample procedure describes how to add a new set of extensions that start with 3 and are 4 digits long. The extension range is from 3000 to 3999.

Procedure

1. Type `change dialplan analysis`.
2. Press `Enter`.

   The system displays the Dial Plan Analysis Table screen.
3. Move the cursor to an empty row.
4. In the **Dialed String** column, type `3`. Press `Tab` to move to the next field.
5. In the **Total Length** column, type `4`. Press `Tab` to move to the next field.
6. In the **Call Type** column, type `ext`.
7. Save the changes.

Defining a multi-location dial plan

Procedure

1. Type display system-parameters customer-options.
2. Press `Enter`.
3. On the Optional Features screen, ensure that the **Multiple Locations** field is y.

   If this field is set to n, the system is not enabled for the Multi-location Dial Plan feature. To enable the feature, go to the Avaya Support website at http://support.avaya.com and open a service request.

   For a complete description of the many Optional Features screens, see *Administering Avaya Aura® Communication Manager*.

Setting up dial prefixes

Procedure

1. Enter `change dialplan analysis`.
2. In the **Call Type** field, type `enb-ext` (enbloc extension). enb-ext represents enbloc extension.
   - If a caller uses enbloc dialing, Communication Manager analyzes the enb-ext entries to determine the route of the call. An example of enbloc dialing is placing a call from a call log.

- If a caller dials a number from the station keypad, Communication Manager does not analyze the enb-ext entries to determine the route of the call.

3. Designate the dial prefix by creating Dial Plan Analysis and UDP entries that incorporate the prefix.

   For information on how to create Dial Plan and UDP entries, see the Adding extension ranges to a dial plan and the Administering the Uniform Dial Plan table.

4. On the Dial Plan Parameters screen, in the appropriate Extension Display Format fields, insert the dial prefix.

   For information on the **Extension Display Format** field, see the *Avaya Aura®* *Communication Manager Screen Reference*.

Related links

Adding extension ranges to a dial plan on page 626
Administering the Uniform Dial Plan table on page 1384

Recommendations for the Dial Plan feature

To derive maximum benefits of the Dial Plan feature, ensure that:

- The maximum length of the prefixed extensions assigned to intercom list is 5 digits. The maximum length is inclusive of the digits of a prefix.
- The maximum length of data-channel extensions is equal to the maximum number of digits that the system supports for an extension. Extensions with an identical first digit may have different lengths. Administering data-channel extensions with the maximum supported length ensures that issues related to time-out for data calls that Communication Manager automatically sets up are avoided. CDR link is an example of the data-channel extension.
- An extension and a FAC contain identical first digits only if the length of the extensions is more, and the extensions are not used to send AAR/ARS faxes.
- Multiple FACs do not contain identical first digits when you create a new dial plan or add information to an existing dial plan. The system distinguishes between FACs with the same first digit by using the **Short Interdigit Timer** value on the Feature Related System Parameters screen.

Interactions for Dial Plan

This section provides information about how the Dial Plan feature interacts with other features.

- Attendant Display and Telephone (Voice Terminal) Display

  Prefixed extensions display without the prefix. Although the telephone does not display the prefix, when you press the return call button, the telephone dials the number with the prefix.

- Integrated Services Digital Network-Basic Rate Interface (ISDN-BRI)

  When an ISDN-BRI station dials a number with additional digits, the station does not recognize the Conference or Transfer buttons. The calling party must delay dialing for 3 seconds or dial # to indicate that the call must route based on the digits already dialed. The station then recognizes the Conference or Transfer buttons and Communication Manager completes the call operation.
- Multifrequency signaling

  Countries that use R2-MFC trunk signaling without Group II tones support flexible numbering. In these countries, if extensions have different first digits, extensions with different lengths are supported.
- Property Management System (PMS)

  Property Management System (PMS) products support a maximum length of 5 digits for extensions. Extensions for PMS are administered on the Dial Plan Analysis screen. If the **PMS Log Endpoint** field and the **Journal/Schedule Endpoint** field on the Hospitality System Parameters (HSP) screen are enabled, Communication Manager supports administration of an extension with a maximum length of 7 digits. This condition on the maximum length of extensions applies even if the Special Application SA8662 is enabled.

  Note:

  If the Dial Plan Analysis screen has extension entries of more than 7 digits, you cannot enter a value in the **PMS Log Endpoint** field and the **Journal/Schedule Endpoint** field. You can administer PMS, PMS_JOURNAL, and PMS_LOG fields on the IP Services screen, but not on the Hospitality System Parameters screen.
- Uniform Dial Plan

  In a DCS environment, to assign extensions from UDP to other servers or switches, the length of extensions must be identical.
- Single-Digit Dialing
  - A prefixed extension contains 5 digits, which includes the digits of the prefix and the digits of the extension.
  - In a dial plan with mixed station numbering, extensions with different lengths can contain 1 to 16 digits.
- Multi-location Dial Plan

The following are the interactions of the Dial plan feature with the Multi-location Dial Plan feature:

- Attendant

  This feature provides a way to administer multiple attendant codes. If you have not administered Attendant Partitioning, Communication Manager supports only one attendant group for each switch. This feature supports Local Centralized Answering Points (LCAP). LCAPs do not require attendant groups to support administration of multiple attendant codes.
- Attendant Vectoring

  If you enable the attendant vectoring feature, this feature takes precedence over existing local attendant codes. Using call vectors, Communication Manager processes attendant

seeking calls or Dial 0 calls. Attendant vectoring is administered by using the local attendant codes and attendant code fields on the Dial Plan screen or the attendant access code field on the Feature Access Code screen.

- Automatic Circuit Assurance

  The field **ACA Referral Destination** on page 1 of the System Features Parameters screen requires the administration of the attendant on the Dial Plan Analysis Table or the attendant access code on the Feature Access Code screen. This field requires that an attendant group exists.

- Automatic Wakeup

  Pending automatic wakeup settings are canceled when you run the **`change extension-station`** command.

- Call Forwarding

  Call forwarding settings are lost when you run the **`change extension-station`** command. If the changed station is a forwarded-to station, you must manually update the extension using the forwarded-to extension.

- Call Park

  Commonly shared extensions cannot park calls because these extensions are not assigned to physical stations. The range of commonly shared extensions can be shared in any location.

- Crisis Alert

  Running the change extension-station command does not update the originating extension on the Crisis Alert System Parameters screen. You have to manually update the originating extension.

- Leave Word Calling (LWC)

  The field **Stations with System-wide Retrieval Permission for the Leave Word Calling Parameters** on page 2 of the System Features Parameters screen requires the administration of the attendant on the Dial Plan Analysis Table screen or the Attendant Access Code on the Feature Access Code screen. This field requires that an attendant group exists.

- Survivable Remote Server

  After you perform the required administration on the main system, you must save the translations to the survivable system. If the translations on the main system and the survivable system are not synchronized, this feature might not function.

- Night Service

  This feature does not work with Location-based Night Service. A customer may want to restrict attendant-seeking calls to attendants who are local to the calling party because the local attendant most likely speaks the same language as the caller. The customer would require an attendant to place only one location in Night Service, without placing the entire switch in Night Service.

  One way to accomplish this is to use hunt groups as attendant queues. You can separately place each hunt group in Night Service and assign each hunt group with its own Night

Service destination. You can administer Night Service destination by tenant, trunk group, or trunk group number.

- Station Hunting

  The station hunting chain is maintained when you run the **change extension-station** command.

- Survivable Remote EPN/WAN Spare Processor

  In a configuration where a survivable remote server exists, if you administer the main system without performing the same administration on the survivable processor, the changes do not reflect on the survivable server when the survivable server takes control. For example, if you run the **change extension-station** command only on the main server, the changed extensions on the server do not reflect on the survivable remote server when the remote processor takes control.

- Uniform dial plan (UDP)

  UDP screens are not updated if you run the **change extension-station** command. External system management tools supported by Avaya handle the UDP table.

The following Communication Manager features, operations, and systems require a user to dial an extension after dialing a Feature Access Code (FAC) or pressing a button. These features support the dial plan extensions of maximum 16 digits in length:

- Add/Remove Agent Skill
- Agent Login/Logout
- Attendant Call Forwarding
- Call Park
- Call Pickup, including Directed Pickup
- Code Calling/Deluxe Paging
- Controlled Restrictions
- EC500 (Extension to Cellular)
- Enhanced Call Forwarding
- Intercom Calling
- Leave Word Calling
- Malicious Call Trace
- Personal Station Access (PSA)
- Posted Messages
- Priority Calling
- Refresh Terminal Parameters
- Remote Access

- Service Observing
- Station Busy Verify
- Terminal Translation Initialization
- Whisper Paging

The following features, operations, and systems also support the dial plan expansion to 16 digits:

- Abbreviated Dialing (AD) – An extension that is stored in an AD button does not change automatically when you change the extension of that station with that extension. If you use the **`change extension-station`** command to change a short extension to a longer extension, you must re-programme an AD button programmed with an extension.
- Application Enablement Services (AES)
- ASAI and CTI API.

  Note:

  Device, Media, and Call Control (DMCC) does not support the extensions of digits in length.
- Attendant Direct Extension Selection (DXS) with Busy Lamp
- Attendant Display
- Attendant Vectoring
- Automatic Call Distribution (ACD)
  - With no reporting
  - With reporting by Basic Call Management System (BCMS)
  - With reporting by Call Management System (CMS), IQ, or Avaya Performance Center
- Automatic Customer Telephone Rearrangement (ACTR)
- Basic Call Management System (BCMS) – Non-EAS agent BCMS/VuStats login IDs can be of maximum 16 digits. Administration of the maximum length of an extension can be done through the **ACD Login Identification Length** field on the Feature-Related System Parameters screen and through the login IDs entered on the BCMS/VuStats Login ID screen.

  Note:

  The BCMS/VuStats login IDs are optional when Expert Agent Selection (EAS) is inactive. If EAS is active, login IDs are required.
- Best Service Routing (BSR) – The **Status Poll** and **Interface VDN** fields in the BSR application tables support 16-digit strings.
- Call Vectoring
- Direct Inward Dialing (DID)
- E911

- Expert Agent Selection (EAS): Logical Agents
- Extension Number Portability (ENP)
- External Reporting Adjunct interface – The external reporting interface messaging protocol Switch Processor Interface (SPI) is enhanced to support the expanded dial plan.
- IP Agent, Release 7
- Multi-Level Precedence and Preemption (MLPP) – The MLPP feature works with short extension dialing in Communication Manager Release 4.0 or later. For a user to be able to dial an MLPP access code followed by a short extension, you must change the **Conv** field on the Precedence Routing Digit Conversion screen to **y**toch. The UDP table converts the short-extension-to-long-extension conversion when you enable the **Conv** field.
- QSIG Message Waiting Indication (MWI) – The DCS/messaging feature does not activate the MWI of stations with extensions that contain more than 7 digits.
- Session Initiation Protocol (SIP)
- Standard Local Survivability (SLS) on G250, G350, G430 and G450 Gateways, and the TGM 550 gateway module
- Meet-Me Conferencing
- VuStats – VuStats displays support longer agent, split, and VDN extensions. To support extensions that contain more than 7 digits, you must update the display formats in Communication Manager Release 3.1 with VuStats Display Formats that supports 7-digit extensions. The system does not update the formats automatically when you increase the extension length.

  Note:

  When longer extensions are used, the fixed 40-character station display cannot accommodate as much other data.

  For more information on BCMS/VuStats Login IDs, see Basic Call Management System (BCMS) earlier in this section.

The following Communication Manager features and operations do not support the dial plan expansion to support extensions with a maximum length of 16 digits:

- Administrable Attendant Access Code: The length of the access code administered through this feature is a maximum of 2 digits.
- Announcements: Recording of the Announcements is not updated to 16-digit dialing and remains at the maximum of 7 digits.
- Basic Communication Management Reporting - Desktop (BCMR-D): This product interfaces with Basic Call Management System (BCMS).
- Distributed Communications System (DCS and DCS+): DCS customers can dial extensions with a maximum of 5 digits. To maintain feature transparency with a longer dial plan, DCS customers must migrate to QSIG.

- Hospitality features, except:
  - Automatic Wakeup: A station with console permissions can enter an Automatic Wakeup request for an extension with a maximum length of 16 digits. The related station display shows only the trailing 7 digits.

    Note:

    No adjustment is made to the number formats that the system sends to the Wakeup Printer. If a Wakeup Printer is administered, extensions longer than 7 digits cannot be administered.
  - Do Not Disturb: A station with console permissions can request the Do Not Disturb feature for extensions with a maximum length of 16 digits. The related station displays shows only the trailing 7 digits.

ISDN-BRI data endpoints: When you add a BRI data endpoint, the **Service Profile Identifier** (SPID) field takes the new extension as the default value. The new extension must not be more than 10 digits. If the endpoint does not support SPIDs, you must disable the Endpoint Initialization feature.

The following are the interactions for the E.164 extension prefixes:

- Abbreviated Dial Button

  A call placed using an Abbreviated Dial (AD) button ignores the Call Type of enb-ext because the AD button can contain the leading digits of a long extension with the remaining digits entered using the keypad.
- Adjunct Switch Applications Interface

  Calls launched by Adjunct Switch Applications Interface (ASAI) are off-switch calls. When ASAI launches a call, the entire calling number is passed to Communication Manager. During routing, Communication Manager considers the calling number as enbloc and considers the Dial Plan enb-ext entries.
- Attendant Feature Invocation

  To invoke the following features, you must dial through UDP to enter the dial prefix before the full extension:
  - Call Forwarding
  - Call Park
  - Code Calling/Deluxe Paging
  - Controlled Restrictions
  - Leave Word Calling/Message Retrieval
  - Refresh Terminal Parameters
  - Station Busy Verify

To invoke the following features, you can enter the full extension that matches an enb-ext entry in the dial plan, or you can include the dial prefix:

- Automatic Wakeup
- Do Not Disturb
- Posted Messages

- You can dial using the keypad or enbloc method from Avaya one-X® Communicator. When you use enbloc dialing, for example, click-to-dial, transmits the digits to its Communication Manager server using Application Enablement Services (AES) or Adjunct Switch Application Interface (ASAI). In absence of AES or ASAI, Avaya one-X® Communicator uses the softphone interface to go off-hook and transmits digits. Avaya one-X® Communicator functions similarly to analog telephones, DCP telephone, and H.323-based telephones.
- Call Coverage – Remote

  If you administer a call coverage destination, the extension can be an enbloc extension, for example, Enhanced Call Forwarding. When a call covers to the call coverage path, Communication Manager considers the covered-to number as enbloc and analyzes the Dial Plan enb-ext entries to determine routing.
- Call Detail Recording

  For outgoing trunk calls:

  - Call Detail Recording (CDR) adjuncts record the originally dialed digits or the transmitted digits.
  - Calling extensions reported to CDR is the administered extension.

  For intra-switch CDR:

  - Called extensions is the administered extension.
  - The prefix digits that must be dialed from a keypad to reach the administered extensions are not supported.
- Call Forwarding

  When a Call Forward destination is entered from a keypad, Communication Manager analyzes the digits to determine the last digit of the dialed number. You must dial through UDP to reach the Call Type enb-ext extension.

  If a Call Forward destination is administered, the extension can be an enbloc extension. When a call is forwarded, Communication Manager processes the forwarded-to number as enbloc and analyzes the Dial Plan enb-ext entries to determine routing.
- Call Management System and Call Center Reporting

  Call Management System and Call Center Reporting provide limited support for extensions that contain more than 7 digits.
- Call Vectors

A Call Vector Route-To destination can be an enbloc extension. When a vector step is executed, Communication Manager considers the route-to number as enbloc and analyzes the Dial Plan enb-ext entries to determine routing.

- Dial Plan Transparency during a Data Network Outage

  Using Dial Plan Transparency, you can dial inter-branch calls during a WAN failure.

- Directed Call Pickup

  When a Directed Call Pickup destination is entered from the keypad, Communication Manager analyzes the digits to determine the last digit of the dialed number. You must dial through UDP to reach the Call Type enb-ext extension.

- Displays

  The E.164 extension prefixes feature has no impact on station displays. In the dial plan, the Call Type enb-ext extension is displayed without any prefix.

- EC500

  Calls launched using the EC500 feature are generally off-switch calls. When EC500 launches a call, the entire calling number is passed to Communication Manager. During routing, Communication Manager considers the calling number as enbloc and considers the Dial Plan enb-ext entries.

- Emergency Calling

  Emergency calling does not function with the Call Type enb-ext extension. In a multinational Communication Manager network, the local ARS and AAR numbering plans are set up to let callers reach an emergency number according to their national routing policy.

- Enbloc DID Trunk Calls

  Trunks that contain the full digit string, do not need to go through the UDP to match on an enb-ext entry in the dial plan. An incoming ISDN SETUP or a SIP INVITE message establishes the calls by using any of the following digit strings:

  - 33-299-31-xx-xx *<the actual extension>*
  - 0299-31-xx-xx *<the UDP version of the extension>*

- H.323 Station Registration

  An H.323 station can register in any of the following ways,

  - Short extension
  - Full extension
  - Prefixed extension

  Avaya recommends that you use the short extension method or full extension method consistently because the backup file with the station settings is stored in a file-based number used during registration. If you use different numbers to log in, the station does not save multiple backup files, which can lead to confusion and inconsistent results.

- Integrated Directory

You can view the administered extension number when you browse the Integrated Directory. Calls launched from the Integrated Directory are processed as enbloc. Communication Manager analyzes the Dial Plan enb-ext entries to determine routing.

- Leave Word Calling

  When a Leave Word Calling destination is entered from a keypad, Communication Manager analyzes the digits to determine the last digit of the dialed number. You must dial through UDP to reach the Call Type enb-ext extension.

- Call Type Digit Analysis

  When a call initiated using the Call Type Digit Analysis feature is considered enbloc. During routing, the Communication Manager server analyzes the Dial Plan enb-ext entries.

- Malicious Call Trace

  When a Malicious Call Trace is activated on behalf of another station from a keypad, Communication Manager analyzes the digits to determine the last digit of the dialed number. To reach the Call Type enb-ext extension, you must dial through UDP.

- Priority Calling

  When a Priority Calling destination is entered from a keypad, the digits are analyzed to determine the last digit of the dialed number. You must dial through UDP to reach the Call Type enb-ext extension.

- Property Management System

  Most Property Management System (PMS) products use the adjunct protocol with extensions not longer than 5 digits. The E.164 feature does not apply to Communication Manager with PMS adjuncts.

- Remote Access

  When a Remote Access FAC is entered from a keypad, Communication Manager checks the digits to determine the last digit of the dialed number. To reach the Call Type enb-ext extension, you must dial through UDP.

- Service Observing

  When an agent extension is entered from a keypad while invoking Service Observing, Communication Manager analyzes the extension to determine the last digit of the dialed number. To reach the Call Type enb-ext extension, you must dial through UDP.

Chapter 73: Dial Plan Transparency

The Dial Plan Transparency feature preserves users' dialing patterns when a gateway registers with a Survivable Remote Server, or when a Port Network requests service from a survivable core server.

Note:

This document uses the term "Survivable Remote Server" in contexts where both Survivable Remote Server and Survivable Core Server scenarios apply. Please keep in mind that Survivable Remote Server accepts registrations from Media Gateways, while Survivable Core Server provides service to Port Networks and Media Gateways.

Detailed Description of Dial Plan Transparency

The Dial Plan Transparency feature automatically completes calls to a called party during an enterprise network outage.

Communication Manager-DPT:

Communication Manager uses the Dial Plan Transparency feature to route calls over a public network when calls cannot be routed over the IP network. The called party or the calling party may not be aware of the network outage situation. For the Communication Manager-DPT (CM-DPT) to work, the same Communication Manager must serve the calling and the called endpoints. To activate CM-DPT, users do not need to change the dialing pattern.

Note:

- The call must be a direct call to the endpoint and not a redirected or a forwarded call.
- CM-DPT is not triggered during a network outage if there are any group features, such as hunt groups, associated with the call.

Session Manager-DPT:

For Session Manager Dial Plan Transparency (SM-DPT) to work, the calling party must be using SIP endpoints, but the called party can use any type of endpoints. The calling and the called endpoints must reside on different Communication Manager servers. Use the SMGR interface to configure SM-DPT on Session Manager and on Communication Manager. You can configure SM-DPT and decide the DPT routing option for each SIP endpoint location.

Note:

- The call can be a direct call, a redirected call, or a forwarded call.
- SM-DPT is not triggered if there are any group features associated with the call.

For more information about SM-DPT, see *Administering Avaya Aura® Session Manager Release 6.3*.

Example of Dial Plan Transparency

The single server distributed systems over IP network and WAN-connected media gateways and port networks have introduced the need for dial plan transparency. When a single server is fragmented into a multiple server configuration, the dial plan transparency becomes a problem. For example, when the media gateway loses contact with the primary controller, the media gateway attempts to re-register with an alternate controller or Local Survivable Processor (LSP).

An LSP might become active for different reasons.

- The network connection between the media gateway and the primary controller fails.
- The primary controller itself fails.

In all the following examples, both the callers are nonIP phones.

In Figure 1, S8300 is the primary controller for six media gateways: MG1, MG2, and MG3 in Network Region 1, and MG4, MG5, and MG6 in Network Region 2. Each media gateway is administered with a primary controller and an alternate controller or a survivable remote server (LSP). LSP1 is an alternate controller for Network Region 1, and LSP2 is an alternate controller for Network Region 2. When a media gateway loses contact with the primary controller, each media gateway attempts to re-register with the LSP. After successful registration, if caller A on MG1 attempts to call caller B on MG6, LSP1 determines whether caller B exists on the originating LSP, the location where caller B resides, and the LDN number for Network Region 2. The LSP places an outgoing trunk call to the LDN for Network Region 2. When one of the media gateways in NR 2 receives the call, DPT is triggered and the call is routed to caller B through an IP inter-gateway connection. In this example, the call is routed from MG1 to MG6.

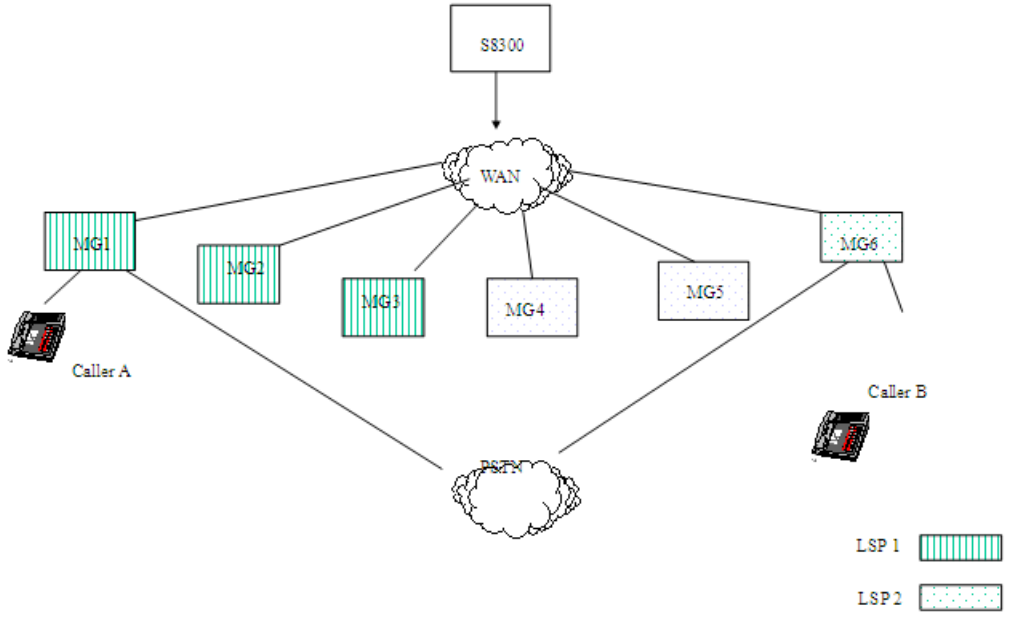


Figure 10: Station-to-Station call between two gateways during network outage

In Figure 2, S8300 is the primary controller for six media gateways: MG1, MG2, and MG3 in Network Region 1, and MG4, MG5, and MG6 in Network Region 2. Each media gateway is administered with a primary controller and an alternate controller or LSP. LSP1 is an alternate controller for Network Region 1, and LSP2 is an alternate controller for Network Region 2. When a network failure occurs, each of the media gateways MG4, MG5, and MG6 loses contact with the primary controller and attempts to re-register with the LSP. In this scenario, if there is a call from PSTN to MG1 for caller B on MG6, S8300 determines whether it can reach caller B through the IP network, determines the Network Region where caller B resides, and places an outgoing trunk call. When a media gateway in Network Region 2 receives a call, DPT is triggered and the call is routed to caller B.

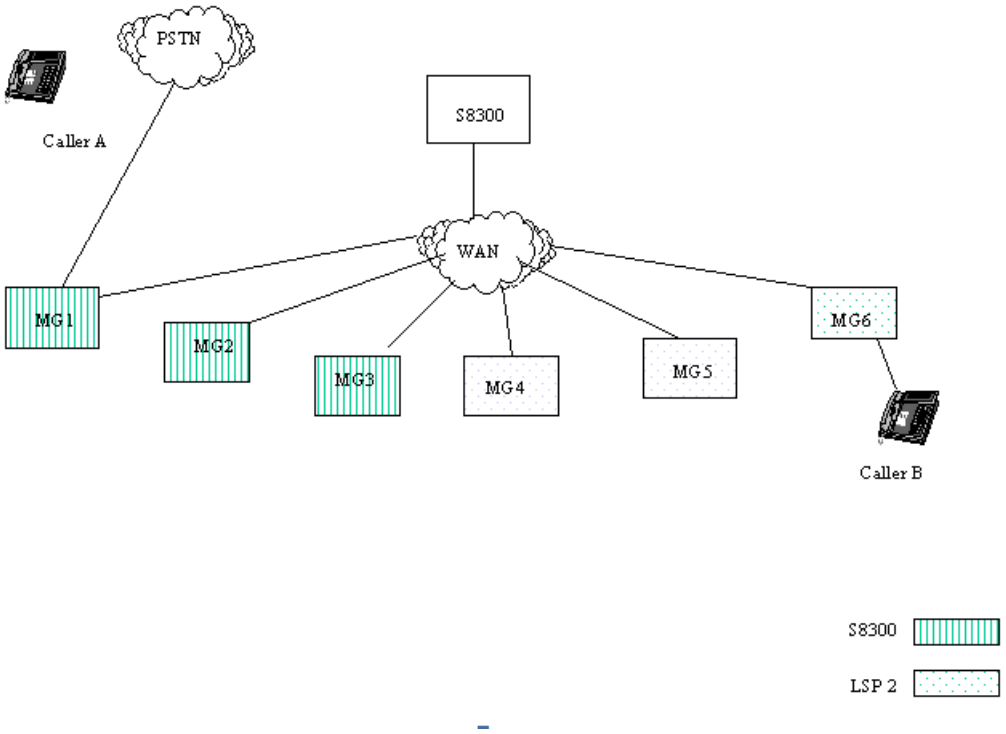


Figure 11: Trunk-to-Station call between main server and gateway during network outage

In Figure 3, S8300 is the primary controller for six media gateways: MG1, MG2, and MG3 in Network Region 1, and MG4, MG5, and MG6 in Network Region 2. Each media gateway is administered with a primary controller and an alternate controller or LSP. LSP1 is an alternate controller for Network Region 1, and LSP2 is an alternate controller for Network Region 2. When a network failure occurs, the media gateway (MG1) loses contact with the primary controller and attempts to re-register with LSP1. In this scenario, if caller A on MG1 attempts to call caller B on MG6, LSP1 determines whether it can reach caller B, determines the Network Region to which caller B belongs, and places an outgoing trunk call. When a media gateway in Network Region 2 receives the call, DPT is triggered, and the call is routed to caller B.

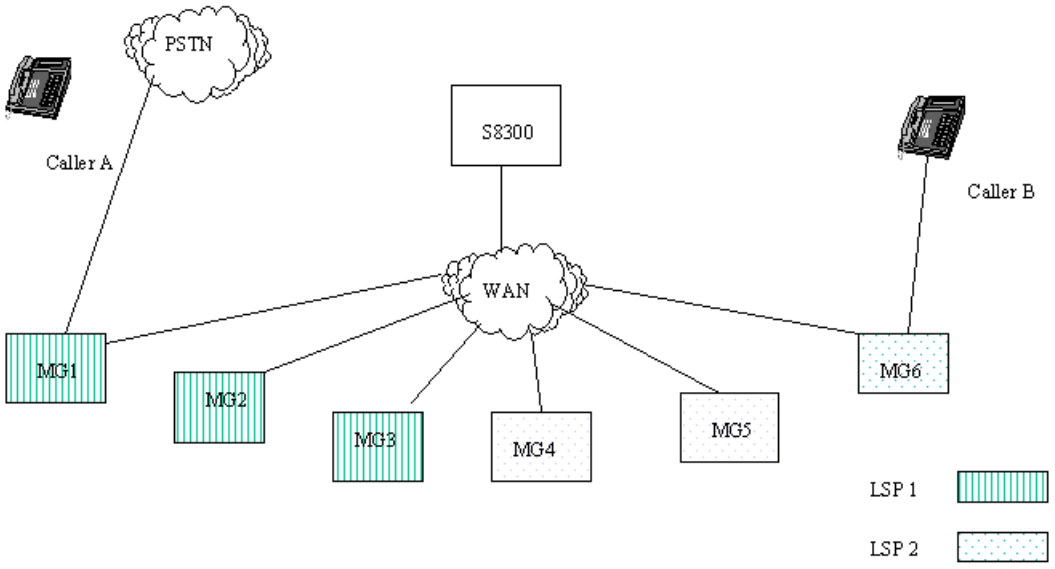


Figure 12: Trunk-to-Station call between two gateways during network outage

Dial Plan Transparency administration

The following step is part of the administration process for the Dial Plan Transparency feature:

- Setting up Dial Plan Transparency

Related links

Setting up Dial Plan Transparency on page 642

Screens for administering Dial Plan Transparency

Screen name	Purpose	Fields	SM-DPT requirement
Feature-Related System Parameters	Turns the feature on or off.	Enable Dial Plan Transparency in Survivable Mode?	No. SM-DPT works even if the field is disabled.
Feature-Related System Parameters	Turns the feature on or off for a particular network region.	Dial Plan Transparency in Survivable Mode?	No. SM-DPT works even if the field is disabled.
IP Network Region	Destination number for incoming PSTN trunk call.	Incoming LDN Extension	Yes. This field must contain the listed directory number.

Table continues…

Screen name	Purpose	Fields	SM-DPT requirement
IP Network Region	Indicates the Class of Restriction for the feature.	COR to use for DPT	No. SM-DPT works even if the field is disabled.
IP Network Region	Makes a listed directory number (LDN) of the destination network region. The ARS table uses this number to route the call to the destination.	Conversion to Full Public Number	No. SM-DPT works even if the field is disabled.
System Parameters-ESS	The community assignments for each Port Network.	Community	No. SM-DPT works even if the field is disabled.

Setting up Dial Plan Transparency

About this task

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

Procedure

1. Type `change system-parameters features`, and press `Enter`.

   The system displays the Feature-Related System Parameters screen. Page down until you see the **SYSTEM-WIDE PARAMETERS** fields.

2. In the **Enable Dial Plan Transparency in Survivable Mode** field, enter `y`.

3. In the **COR to Use for DPT** field, enter the Class of Restriction to use for Dial Plan Transparency.

   The default is station, where the FRL of the calling station determines whether that station is permitted to make a trunk call and if so, which trunk(s) it is able to access.

4. Type `change ip-network region` *n*, where *n* is the number of the Network Region to change. Press `Enter`.

   The system displays the IP Network Region screen. Page down until you see the **INTER-GATEWAY ALTERNATE ROUTING/DIAL PLAN TRANSPARENCY** fields.

5. In the **Incoming LDN Extension** field, If not already done for IGAR, allocate one incoming DID/LDN extension for incoming DPT calls.

   This extension can be shared by IGAR and DPT – the system will distinguish incoming IGAR calls from incoming DPT calls.

6. In the **Dial Plan Transparency in Survivable Mode** field, enter `y`.

7. Ensure that each IGAR/DPT-enabled Network Region has sufficient trunks for the expected number of outgoing and incoming DPT calls.

There is no need to set the maximum number of trunks for DPT.

8. Use existing routing techniques to ensure an outgoing DPT call from a given Network Region will have access to an outgoing trunk.

   Unlike IGAR, the outgoing trunk need not be in the same Network Region as the calling endpoint, as long as the endpoint and trunk Network Regions are interconnected.

9. If you are setting up DTP for a Survivable Core Server, type `change system-parameters ess`. Press `Enter`.

   The system displays the System Parameters-ESS screen. Page down to page 6.

10. In the **Community** field, enter the community assignments for each Port Network.

    Assigning a Survivable Core Server to a community associates the Survivable Core Server with the IPSI(s) (IP Interface Server) in the Port Network(s) for that community. The association effects how the Survivable Core Server is prioritized for the IPSI in that community, if the Survivable Core Server is administered with a Local Preferred or Local Only preference.

    Note:

    For more information on Survivable Core Server, see *Avaya Aura® Communication Manager Survivable Options*.

Maintenance for Dial Plan Transparency

DPT Alarms

Alarms should already exist when an Survivable Remote Server or Survivable Core Server becomes active. No new alarms are introduced when a gateway goes into Survivable Remote Server mode.

DPT Audits/Logging

As with IGAR and most other features, Communication Manager logs Denial Events to help debug cases when a DPT trunk call cannot be initiated.

DPT Debugging/Diagnostic Tools

For calls that are initiated but do not terminate properly, tools such as List Trace, List ARS Route-Chosen, Call Detail Recording, and Message Sequence Tracer can help diagnose the problem. List Trace shows the outgoing trunk call placed on behalf of the user when DPT is invoked.

Considerations for Dial Plan Transparency

This section provides information about how the Dial Plan Transparency (DPT) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Dial Plan Transparency under all conditions. The following considerations apply to Dial Plan Transparency:

- DPT only handles WAN connectivity failures between Network Regions. DPT does not cover the following cases:
  - Two Gateways in the same Network Region, registered to the same server (main or Survivable Remote Server or Survivable Core Server), cannot reach each other due to LAN congestion or failure. Note that this case cannot be handled by IGAR either.
  - A Gateway becomes disconnected from the main server and cannot register with an Survivable Remote Server or Survivable Core Server at all. In such a case the gateway will enter Standard Local Survivability mode, which provides basic call processing functionality during the outage.
- Failover strategies for Gateways and Port Networks, and alternate gatekeeper lists for IP stations must be in harmony. DPT does not work in the following scenarios:
  - Two Gateways or Port Networks in the same Network Region register to different Survivable Remote Server or Survivable Core Server servers during a network outage.
  - Two IP endpoints in the same Network Region register to different servers during a network outage.
- Because DPT calls are trunk calls, most station features cannot be supported. DCS and QSIG features are not supported, even if the trunk carrying the DPT call supports DCS or QSIG. Communication Manager displays a new reason code to alert users about the reduced functionality.

Fiber PNC with Remote PNs DPT Considerations

Fiber PNC refers to a Center-Stage Switch, ATM-PNC, DS1C-PN. Please note the following:

- Customers wanting DPT for Survivable Core Server-controlled Port Networks (PNs) must migrate those PNs from Fiber-PNC to IP-PNC. Fiber-connected cabinets must be in Network Region 1.
- Fiber-PNC users can reach disconnected users in other Network Regions through DPT.
- IP-PNC/GW can only initiate DPT calls to the fiber-PNC fragment that contains the trunks associated with the IGAR LDN.
- Users connected through Fiber-PNC cannot use DPT if another fiber PN fails over to different Survivable Core Server. This is because DPT is not triggered within same Network Region.

Interactions for Dial Plan Transparency

This section provides information about how the Dial Plan Transparency (DPT) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Dial Plan Transparency in any feature configuration.

Because DPT calls are trunk calls, many Communication Manager features cannot be supported. DCS and QSIG features are not supported, even if the trunk carrying the DPT call supports DCS or QSIG (including SBS), because the call is not being originated in the normal way.

When you set up a multi-gateway server, it is unlikely that they will set up and maintain a DCS or QSIG net-work in parallel to support feature transparency in case of network fragmentation. Therefore, the only ways to get additional features to work are (1) in-band signaling over the DPT trunk before ringing the called party, or (2) out-of-band signaling using Q.931 messages. However, In-band signaling delays call setup, and Out-of-band signaling do not work over normal public network ISDN connections.

AAR/ARS partitioning

ARS partitioning is used when routing the DPT trunk call, if the station COR is used to route the call. If not, then ARS Partition 1 is used.

Abbreviated Dialing

DPT is invoked whether the caller dials using the keypad or by pressing an Abbreviated Dialing button.

Alternate facilities restriction levels

If the calling station has invoked its Alternate facilities restriction level (FRL) and the station COR is used to route the call, the Alternate FRL is used.

Announcements

External announcements are not supported if the adjunct does not have access to the Survivable Remote Server.

Attendants

Calls to or from an attendant invoke DPT.

Authorization Codes

If the station COR is used to route DPT calls, and a caller’s FRL is not high enough to access a Route Pattern Preference, and authorization codes are enabled, then the caller is prompted to enter an authorization code. This might be a surprise to some callers, but those with displays will recognize the reason for the prompting. If the unrestricted COR is used to route DPT calls, the call routes without prompting the caller.

Automatic Callback

Automatic callback (ACB) is not supported when the initial call has routed through DPT, even if the DPT call routes over a DCS or QSIG trunk group with TSCs enabled.

ANI

If an incoming ISDN call is routed using DPT, and the outgoing DPT call also travels through ISDN, the Calling Party Number IE received on the incoming call is passed on with the DPT call, and that number is displayed to the called user. It is under investigation to what extent this works with other trunks that provide Caller ID such as MFC trunks.

ARS

ARS is used to route DPT calls. The user must administer the ARS analysis forms to support Dial Plan Transparency for Survivable Remote Server and Survivable Core Server fragments.

Bridging

Bridged appearances within a Survivable Remote Server fragment will function properly. However, bridging is not supported across Survivable Remote Server fragments, so DPT cannot be invoked by means of a user pressing a bridged appearance button.

If a server becomes active in Survivable Remote Server mode and bridged appearances exist across Survivable Remote Server fragments, bridging is not supported. For calls that originate from a call appearance with a bridged extension not local to the Survivable Remote Server, the bridged extension does not show/have access to the call. Calls cannot originate on a bridged extension if the principal extension is not local to the Survivable Remote Server. For incoming calls to an extension on a Survivable Remote Server, the bridged extension does not alert if it is not local to the Survivable Remote Server.

Busy Indicator

The busy indicator button is not supported across disconnected network fragments.

Call Detail Recording

CDR records are stored in a buffer while in Survivable Remote Server mode. Since the CDR adjunct is administered on the main server, no data can be sent to the adjunct from the Survivable Remote Server. Therefore, if the CDR buffer hits its capacity, CDR records are overwritten and data is lost.

Call Forwarding

Several scenarios must be considered. Assume the parties involved are A, B, and C, where A calls B, and B is forwarded to C.

- A and B are in the same Network Region; C is in a Network Region accessible only through DPT. This is not a principal termination and so DPT is not invoked – instead, the call either follows B’s coverage path, or busy tone is played back to A.
- B and C are in the same Network Region. A can access B only through DPT. DTP is not invoked — instead, the call either follows B's coverage path or busy tone is played back to A.
- If A, B, and C are all in Survivable Remote Server fragments, the result is a combination of the above two cases, and the first one overrides – the call is not forwarded from B to C, but either follows B’s coverage path, or busy tone is played back to A.

Call Park

Call parking is not supported between disconnected network fragments.

Call Pickup

Call pickup is not supported across disconnected network fragments.

Conference

Conferencing is supported while in Survivable Remote Server mode, but the count of conference parties is different. That is, if two parties on a conference are in the Survivable Remote Server and two are on the main server, each station sees CONFERENCE 2, meaning each side is only aware of three parties on the conference: the two stations and the DPT trunk.

Note also that the system does not optimize trunk connections (as happens with IGAR), nor are the DCS or QSIG Path Optimization features available. Therefore, a conference call could use up many more trunks than are actually necessary; users would have to recognize the Survivable Remote Server condition (perhaps because of the reason code on their display) and would have to optimize trunk usage “manually” (for example, by conferencing together parties in the same Survivable Remote Server fragment).

Coverage

Call coverage is not a principal termination, so Communication Manager 4.0 or later does invoke DPT, even if the call is covering to a voice mail adjunct. That is, if A calls B, and B normally covers to C, there are two cases:

- If C is accessible to B, coverage takes place and C rings. “Accessible” means that the server controlling B’s gateway also controls C’s gateway.
- If C is not accessible to B, then the call rings forever at B. To get the call to cover to C in this case, the customer must use the Remote Coverage solution.

  In the latter case, if A and B are not controlled by the same server, Remote Coverage through a trunk is initiated by B’s server, not A’s server.

Crisis Alert

The Crisis Alert feature causes Communication Manager to alert an attendant when an emergency call is placed. As described elsewhere, DPT does not alert members of an attendant group in a disconnected gateway. However, attendants accessible to the caller are alerted.

E911

Calls to an emergency number such as 911 in North America work normally, since those calls generally travel out over trunks local to the caller’s home gateway. We do not expect DPT to be invoked.

EC500

An incoming DPT call can invoke EC500 – that is, it can generate a trunk call to a cell phone or other re mote endpoint – assuming outgoing trunks are available on the server controlling the called party.

Group Paging

Group Paging is not supported across Survivable Remote Server fragments.

Hunt Groups

Calls to hunt groups are not supported between Survivable Remote Server fragments. The problem with supporting hunt groups is the unknown state of the members in the hunt group. For example, you may know that the station is OOS because you are in Survivable Remote Server mode, but you don’t know if that station is on another call since you no longer have control of it.

The ports in a Voice Mail hunt group seldom span gateways. The Remote Coverage solution described elsewhere addresses calls that are placed directly to, or that cover to, a Voice Mail hunt group whose ports are in a disconnected gateway (typically on the main server).

Intercom

Intercom calls are not support between Survivable Remote Server fragments.

IP Endpoints

Because an IP endpoint does not have a physical port, Communication Manager software cannot be as sure as with digital or analog endpoints what Network Region it belongs to.

With an IP Softphone, the problem is even more acute. A Telecommuter or Road Warrior using an IP Softphone may log in and out several times during a WAN outage and register with different servers (the main or an Survivable Remote Server or Survivable Core Server). Thus, an IP Softphone's Last Network Region may be out of date, causing Communication Manager software to route DPT calls to that Softphone using the LDN of the wrong Network Region. If that wrong Network Region is disconnected from the actual Network Region of the Softphone, the call will fail. (By contrast, if the wrong Network Region happens to be connected to the actual Network Region, the call will succeed.)

In such a case, the Telecommuter or Road Warrior may need to give an alternate PSTN number at which they can be reached. Outgoing calls from an IP Softphone registered to an Survivable Remote Server or Survivable Core Server trigger DPT and work properly.

Last Number Dialed

DPT is invoked whether the caller dials using the keypad or by pressing a **Last Number Dialed** button.

Leave Word Calling

Leave Word Calling (LWC) is not supported when the initial call has routed through DPT, even if the DPT call routes over an SDN/DCS+ trunk group. To get LWC to work over an SDN/DCS+ trunk group, the customer would have to be using 4-digit or 5-digit UDP dialing and have TSCs enabled. But such a customer does not really need DPT, because they get better efficient transparency among their gateways without it.

Note that LWC is used primarily by Voice Mail systems that use Digital Set Emulation (that is, they simulate a DCP endpoint). They use the LWC Store and LWC Cancel Feature Access Codes to light and turn off message waiting lamps.

Loudspeaker paging

Loudspeaker paging is not supported between Survivable Remote Server fragments.

Malicious Call Trace

If the recipient of a DPT call invokes Malicious Call Trace (MCT), the results visible to the MCT Controller and on the MCT History log are the same as for an incoming trunk call. The identity of the calling station is not displayed.

Meet-me Conference

Each Survivable Remote Server or Survivable Core Server has its own "copy" of a Meet-Me Conference VDN and vector when a system breaks up due to a WAN outage. Thus, callers in disconnected gateways may dial into the "same" Meet-me Conference (MMC), but these are

separate conferences. Since an MMC does not have a physical port or Network Region, DPT is not triggered to merge these conferences together.

Message Retrieval

Retrieval of Leave Word Calling messages is not supported while in Survivable Remote Server/ Survivable Core Server mode if the messages are stored in a remote Voice Mail server (typically Communication Manager Messaging).

Multi-Level Precedence and Preemption

The caller's precedence level is not transmitted when DPT initiates a trunk call. Therefore, a high-ranking caller that invokes DPT will not preempt an existing trunk call, nor will a high-ranking caller placing a precedence call preempt a trunk call initiated by DPT.

No-Hold Conferencing

A call initiated by the No-Hold Conferencing (NHC) feature triggers DPT. As soon as the DPT signaling has completed, the trunk is conference into the call and the parties hear the normal conference tones (if applicable).

Personal Station Access

During network fragmentation, an Survivable Remote Server or Survivable Core Server is not notified about users on remote gateways associating their stations using PSA. Thus, DPT is not triggered on a call to a station that was associated through PSA during the outage.

Priority Calling

A Priority Call can invoke DPT, but the called party does not ring with the Priority (typically 3-burst) ring pattern, even if the DPT call routes over a DCS or QSIG trunk group.

Service Observing

A user cannot use Service Observing to monitor a user served by a disconnected Survivable Remote Server or Survivable Core Server. Remote Service Observing works, but the observer must be notified that the network has fragmented before knowing to invoke Remote Service Observing.

Station Lock

Locking a station changes its COR. Thus, if the Station Lock COR blocks outgoing trunk calls, and the COR to Use for DPT system parameter is set to station, then the locked station cannot make DPT calls, while the unlocked station can do so.

TTI

During network fragmentation, a Survivable Remote Server or Survivable Core Server is not notified about users on remote gateways associating their stations using TTI. Thus, DPT will not be triggered on a call to a station that was associated through TTI during the outage.

Transfer

A call initiated as part of a transfer operation can trigger Dial Plan Transparency. This includes all types of transfer (station & attendant, normal & pull transfer, and so on).

Transfer into/out of Voice Mail

A call initiated as part of a Transfer out of Voice Mail operation can trigger DPT – it looks like a normal call placed by a QSIG trunk or hunt group member.

Transfer into Voice Mail sets up a call to the Voice Mail Hunt Group, all of whose members are out of service during network fragmentation. It can be made to work by assigning a Coverage Path to the Hunt Group – see the subsection on Voice Messaging.

Voice Messaging

Retrieving Voice Messages:

A user may dial the internal extension of the Voice Mail Hunt Group to access/retrieve voice messages on a QSIG-connected VM server or a Communication Manager Messaging server. Without any special changes, doing so will result in busy tone, because the hunt group or QSIG trunk group members are out of service from the point of view of the Survivable Remote Server or Survivable Core Server. Thus, users must have a way of automatically dialing “out” through the PSTN to the VM server while their Gateway is served by an Survivable Remote Server or Survivable Core Server.

This can be done by assigning a Coverage Path to the Voice Mail Hunt Group itself, with a special Remote Coverage point that is only active when the caller is on a Gateway in Survivable Remote Server or Survivable Core Server mode.

Message Waiting Lamps:

Note that whenever the Gateway is disconnected from the VM server, Message Waiting lamps are stuck in the on or off state until the Gateway reregisters, and the VM server updates the lamps.

Whisper Paging

A call initiated as part of a Whisper Paging operation can trigger DPT.

Chapter 74: Distinctive Ringing

Use the Distinctive Ringing feature to distinguish between incoming call types based on the ringing pattern of the call.

Detailed description of Distinctive Ringing

For multiappearance telephones, you can administer the system-wide distinctive-ringing cycles. You cannot administer system-wide distinctive-ringing cycles for single-line analog telephones. For single-line analog telephones, you must administer the ringing cycle for the user on a Station screen. For more information, see the Personalized Ringing feature.

Most installations use a one-burst ring for internal calls, a two-burst ring for external calls, and a three-burst ring for priority calls.

The system controls the ringing cycles for the following types of calls. You can administer ringing for:

- Automatic and Dial Intercom calls
- Manual Signaling calls
- Redirect Notification calls

If the user of an internal telephone transfers an external call, the call usually rings as an internal call. You can administer the system so that the transferred call rings as an external call.

The alerting patterns of the stations depend on the administration of **Distinctive Audible Alert**. When Tenant Partitioning is disabled, the system parameters-features screen displays **Distinctive Audible Alert**. When Tenant Partitioning is enabled, the Tenant screen displays **Distinctive Audible Alert**.

Distinctive Ringing administration

The following step is part of the administration process for the Distinctive Ringing feature:

- Defining Distinctive Ringing

Related links

Defining Distinctive Ringing on page 652

Screens for administering Distinctive Ringing

Screen name	Purpose	Fields
Feature-Related System Parameters	Assign the number of rings for different types of calls in the **Distinctive Audible Alerting** area.	• Internal • External • Priority
	Change the ringing pattern for an internal call to the ringing pattern of an external call, when a user or an attendant transfers the internal call.	Update Transferred Ring Pattern
	Specify the type of an attendant originated call.	Attendant Originated Calls
Tenant	Assign the number of rings for different types of calls in the **Distinctive Audible Alerting** area.	• Internal • External • Priority
	Specify the type of an attendant originated call.	Attendant Originated Calls
Station	Assign the Distinctive Alerting feature to the station.	Distinctive Audible Alert

Defining Distinctive Ringing

Procedure

1. Check for Tenant Partitioning.
   - If Tenant Partitioning is disabled, type `change system-parameters features`.
   - If Tenant Partitioning is enabled, type `change tenant n`, where `n` is the tenant number.
2. Press `Enter`.
3. Click **Next** until you see the **Distinctive Audible Alerting** area.
4. In the **Distinctive Audible Alerting** area, perform the following actions:
   - In the `internal` field, type the number of rings you want the system to use for an internal call.
   - In the `external` field, type the number of rings you want the system to use for an external call.
   - In the `Priority` field, type the number of rings you want the system to use for a priority call.
   - In the `Attendant Originated Calls` field, type the ring pattern you want the system to use for calls originated by an attendant.

5. Select `Enter` to save the changes.

Updating ring pattern

Procedure

1. Type `change system-parameters features`.
2. Press `Enter`.
3. On the System-parameters features screen, click **Next** until you see the **Update Transferred Ring Pattern** field.
4. In the **Update Transferred Ring Pattern** field, perform one of the following actions:
   - If you want the system to change the ringing pattern for an internal call to the ringing pattern of an external call, when a user or an attendant transfers the call, type `y`.

     If most of your calls go through an attendant, you might want to set this field to `y` so that your users can identify an external call.
   - If you do not want the system to change the ringing pattern for an internal call to the ringing pattern of an external call, when a user or an attendant transfers the call, type `n`.
5. Select `Enter` to save the changes.

Considerations for Distinctive Ringing

This section provides information about how the Distinctive Ringing feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Distinctive Ringing under all conditions. The following considerations apply to Distinctive Ringing:

- If Distinctive Ringing is disabled, the system generates a one-burst repetitive tone for all incoming calls. The one-burst repetitive tone is useful for equipment that is interfaced by analog lines, especially if you use an off-premises telephone. A single distinctive ring cycle is used for each new incoming call to an off-hook telephone or headset. The system alerts a Callmaster® terminal with a single ring cycle whenever either the headset or the handset is plugged into the headset jack.

Interactions for Distinctive Ringing

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

Personalized Ringing

The called party hears the user-selected ringing pattern for the distinctive ring cycles.

Chapter 75: Do Not Disturb

Using Do Not Disturb, guests, attendants, and authorized front-desk phone users (those with console permission) can request that no calls, other than priority calls, terminate at a particular extension until a specified time. At the specified time, the system automatically deactivates the feature and calls terminate normally at the extension.

Detailed description of Do Not Disturb

Do Not Disturb is a form of termination restriction associated with an automatic deactivate time. When Do Not Disturb is active, the user receives only those calls associated with Automatic Callback, Automatic Wakeup, and Priority Calling, and those calls that are redirected to that extension via the Call Coverage and Call Forwarding All Calls. All other calls redirect to a recorded announcement, an attendant, or intercept tone. Communication Manager can be set to give a special dial tone whenever an analog set goes off-hook when Do Not Disturb is active.

Phone users with touch-tone dialing can activate this feature themselves or ask the front desk to do it for them. Users with rotary-dial phones must call the attendant or front-desk user to request Do Not Disturb.

Activation by phone users

Phone users can activate Do Not Disturb by dial access or by button access.

Dial Access

When a user dials a Do Not Disturb FAC, the system prompts the user to enter a deactivate time. The user may later change or delete the request by dialing the Do Not Disturb FAC again and entering the required information.

If the user makes invalid entries or if system conditions prevent entry of the request, the system informs the user to dial the attendant or front desk for assistance.

Button Access

If a phone has a Do Not Disturb button, the user can press the button to activate the feature. The handset may be on-hook or off-hook. The user presses the button a second time to deactivate the feature.

The lamp associated with the Do Not Disturb button lights until the feature is deactivated with the button. An automatic-deactivate time is not provided.

Activation by attendant

The attendant can activate the feature for a user or a group of users. (The assigned COR determines which users are in the group.) The attendant presses the Do Not Disturb — Extension button followed by the extension, or the Do Not Disturb — Group button. The extension followed by the appropriate COR number.

The attendant can cancel a Do Not Disturb request by activating the feature, entering the required extension or group COR number, and pressing the delete button.

Activation through a PMS

The system provides an interface to a PMS. This interface activates and deactivates controlled restrictions. Activation of Do Not Disturb through a PMS is similar to activation of termination restriction. A scheduled deactivate time cannot be specified.

Audit Trail Reports

The system keeps a record of all phones that are in Do Not Disturb mode. You can display or print this information.

Administer the following reports for printing on a daily basis:

- Do Not Disturb Status Report — This report lists all extensions with Do Not Disturb active and the specified deactivate time for each.
- Do Not Disturb Plus COR Status Report — This report lists all extensions, plus those whose controlled-restriction level is termination restriction. (The attendant activates termination restriction for a specific extension or COR. A deactivate time is not associated with termination restriction.)

Records do not include Do Not Disturb information for extensions that are both termination and outward restricted.

Considerations for Do Not Disturb

This section provides information about how the Do Not Disturb feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Do Not Disturb under all conditions. The following consideration apply to Do Not Disturb:

- A front-desk user must have a console-permission COS to activate this feature.

Interactions for Do Not Disturb

This section provides information about how the Do Not Disturb feature interact with other features on the system. Use this information to ensure that you receive the maximum benefits of Do Not Disturb in any feature configuration.

Automatic Callback

Do Not Disturb does not block an Automatic Callback call. Return calls terminate at a phone in the normal way.

Automatic Wakeup

An Automatic Wakeup call deactivates Do Not Disturb and alerts the guest at the specified time.

Call Coverage

If a point in a coverage path has Do Not Disturb active, calls covering to that extension alert the extension unless the extension has controlled-restriction termination active. When Do Not Disturb is active and a phone does not have a coverage path, calls are routed to the attendant.

Call Forwarding All Calls

If Do Not Disturb is active at the forwarding extension, the caller receives intercept treatment. If Do Not Disturb is active at the forwarded-to extension, the call alerts the forwarded-to extension.

Controlled Restriction

When a phone has total-controlled restriction, it cannot receive or place any calls. However, it can receive a call if another station has an auto-icom button pointing to the controlled-restriction station.

Internal Automatic Answer (IAA)

Activation of Do Not Disturb at the called phone preempts IAA.

PC Console

You cannot implement Do Not Disturb at a PC Console.

PMS Interface

Checkout from either a PMS or Communication Manager automatically deactivates Do Not Disturb for the specified extension.

Chapter 76: EC500 in-call feature invocation

With this feature, you can enable EC500 users to use in-call features, such as Hold and consult, Transfer, and Conference. To enable the in-call features, users must dial Feature Access Code (FAC) that you have configured.

EC500 in-call feature invocation supports the out-of-band and rtp-payload digit detection mechanism. Communication Manager supports this detection only on H323 and SIP trunks.

You must administer Avaya Aura® Media Server or Branch Gateway as media resource on Communication Manager.

You must configure a large number of media resources with Communication Manager to support EC500 calls on local media resources. Otherwise, the total number of simultaneous calls supported are reduced. If no media resources are available, Communication Manager logs the `No channel resources` denial event.

Communication Manager transmits all FAC digits to the far-end signaling group by using the end-to-end signaling to provide information to applications such as voice mail. The required digits for the application are in conflict with the FAC. Therefore, you must configure FAC so that it does not conflict with other applications.

Important:

When you configure the Feature Access Code with EC500, Feature Access Code should not conflict with any other applications such as voice mail, which expects in-call DTMF digits.

Screens for administering EC500 in-call feature invocation

Screen name	Purpose	Fields
STATIONS WITH OFF-PBX TTELEPHONE INTEGRATION	To view the EC500 configuration number.	**Config set**
CONFIGURATION SET	To enable EC500 in-call feature invocation.	**Feature Invocation by In-call DTMF Code**
SIGNALING GROUP	To configure DTMF over IP.	**DTMF over IP**

Table continues…

Screen name	Purpose	Fields
MEDIA-GATEWAY REPORT	To verify the firmware.	**Serial No/FW Ver/HW Vint/ RecRule**
Off-Pbx Telephone features	To configure Off-Pbx feature access codes.	• **Hold and Initiate New Call** • **Transfer Complete** • **Conference Complete** • **Toggle With Held Call** • **Cancel Current Call**

Viewing the EC500 configuration number

Procedure

1. On the Communication Manager CLI, type `display off-pbx-telephone station-mapping`.
2. On the STATIONS WITH OFF-PBX TELEPHONE INTEGRATION screen, view and note the value in the **Config Set** field.

Enabling EC500 in-call feature invocation

Procedure

1. On the Communication Manager CLI, type `change off-pbx-telephone configuration set n`.

   n is the value of the **Config set** field that you have noted in the “Viewing the EC500 configuration number” procedure.
2. On the CONFIGURATION SET screen, in the **Feature Invocation by In-call DTMF Code** field, type `y`.
3. Save the changes.

Configuring DTMF over IP for the EC500 signaling group

Procedure

1. On the Communication Manager CLI, type `change signaling-group n`.

   n is the EC500 signaling group.
2. On the SIGNALING GROUP screen, in the **DTMF over IP** field, type one of the following:

   • `rtp-payload`

   • `out-of-band`
3. Save the changes.

Verifying the Branch Gateway firmware

Procedure

1. On the Communication Manager CLI, type `list media-gateway`.
2. On the MEDIA GATEWAY REPORT screen, verify that the value of the **Serial no/FW Ver/HW Vint/RecRule** field for Branch Gateway is **40.2.0** or greater.

   If the value is less than **40.2.0**, upgrade the firmware. For more information, see *Deploying and Upgrading Avaya G450 Branch Gateway* or *Deploying and Upgrading Avaya G430 Branch Gateway*.

Configuring Off-PBX feature access codes

Procedure

1. On the Communication Manager CLI, type `change feature-access-codes`.
2. On the Off Pbx Telephone Features screen, type the feature access codes in the following fields:
   - **Hold and Initiate New Call**
   - **Transfer Complete**
   - **Conference Complete**
   - **Toggle With Held Call**
   - **Cancel Current Call**
3. Save the changes.

Interaction

This section provides information about how EC500 in-call feature invocation interacts with other features in Communication Manager.

Digit collection

If you enable any digit collection feature, such as the vector digit collection step, Communication Manager deactivates the EC500 in-call feature invocation until the call is delivered to the user.

Enterprise Mobility eXperience (EMX)

If the EC500 applications are added to a primary station, the Avaya Workplace Client cannot create EMX applications for the same primary station.

Similarly, if a Avaya Workplace Client has created EMX applications for a primary station, you cannot add EC500 applications for the same primary station.

Limitations

Communication Manager does not support EC500 in-call feature invocation on the following:

- Time-Division Multiplexing (TDM) trunks, such as ISDN-PRI.
- Port Networks and older Branch Gateway instances.
- If the set type of your station is SIPCC, and an agent is logged on to the station with SIPCC, and the current call is ACD call, then the EC500 feature does not work.

Chapter 77: Emergency Calls from Unnamed IP Endpoints

Use the Emergency Calls from Unnamed IP Endpoints feature to register an IP telephone without an extension number. The Emergency Calls from Unnamed IP Endpoints feature places the IP telephone into Terminal Translation Initialization (TTI) service. Users can dial a Feature Access Code (FAC) to either associate an extension number with a telephone, or to dissociate an extension number from a telephone.

A person can use an IP telephone that is in TTI service to make emergency calls if Communication Manager is appropriately administered.

Note:

Check with your Avaya sales representative or your Avaya Authorized Business Partner for availability of this feature.

Detailed description of Emergency Calls from Unnamed IP Endpoints

Without the Emergency Calls from Unnamed IP Endpoints feature, if a user of an IP telephone registers the extension to another telephone or softphone, the IP telephone changes to an unregistered state. The IP telephone cannot reregister until the user releases the extension number from the other telephone or softphone. A user cannot use an IP telephone that is in an unregistered state to make emergency calls.

However, if a user has a DCP telephone and registers the extension to another telephone or softphone, the DCP telephone goes into a dissociated state. In this state, a user can still use the DCP telephone to make emergency calls if Communication Manager is appropriately administered.

The Emergency Calls from Unnamed IP Endpoints feature makes IP telephones work like DCP telephones when users make emergency calls from telephones that do not have extension numbers.

When an IP telephone is plugged in, power cycled, or after a user logs off, the system displays a prompt on the telephone display. The prompt asks the user for an extension number and a

password. If a user does not dial at least one digit within 60 seconds from when the system displays the first prompt, the system registers the telephone into TTI service.

If a user wants to make an unnamed IP telephone reregister with an extension, the user must either:

- Press the `Login` prompt on the telephone softkey, and then enter an extension and a password
- Use the Feature Access Code (FAC) for the Personal Station Access (PSA) Associate feature

  A user can dial the FAC for the PSA Associate feature from an IP telephone that is in TTI service only if one of the following conditions is true:

  - the **Receive Unencrypted from IP Endpoints** field on the Security-Related System Parameters screen is set to y
  - The telephone encrypts signaling

    If a user dials the FAC for the PSA Disassociate feature, the system immediately places the IP telephone into TTI service.

The Emergency Calls from Unnamed IP Endpoints feature does not work with the following IP telephones:

- Non-AVAYA H.323 IP telephones
- IP Softphone release 5 or earlier
- IP telephones with 2.1 firmware or earlier
- IP telephones with 2.5 firmware

The Emergency Calls from Unnamed IP Endpoints feature supports the following capabilities:

- If a person makes a call from an IP telephone that is in TTI service, the called party sees the IP port of the calling party and the words “TTI port” on their display telephone. For example, a called party might see S00001 TTI port on their display telephone. Using this display, the called party can identify the source of the call.
- If the Malicious Call Trace (MCT) feature traces an IP telephone that is in TTI service, the MCT controller displays the IP port. The administrator can use the **`display port n`** command to convert the port into an IP address. The administrator can then learn the original extension of the IP telephone, and where the telephone is located.

These two capabilities are especially helpful to trace calls.

The system can register an IP telephone to TTI service only if that IP telephone has an IP address that is administered on the IP Address Mapping screen.

The system displays the IP address of an IP telephone that is in TTI service in the **Identification** field on the Port Information screen.

Emergency Calls from Unnamed IP Endpoints administration

This section describes the prerequisites and the screens for the Emergency Calls from Unnamed IP Endpoints feature.

Preparing to administer Emergency Calls from Unnamed IP Endpoints

Procedure

1. On the Optional Features screen, ensure that the **G3 Version** field is set to V13 or later.

   V13 is the version for Communication Manager Release 3.0. If this field is not set to V13 or later, your system does not support the Feature Description and Implementation feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Emergency Calls from Unnamed IP Endpoints, or to open a service request.

   To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

2. The Emergency Calls from Unnamed IP Endpoints feature requires that the TTI for voice terminals option be turned on.

   Your license file sets this field. If the TTI for voice terminals option is turned off for your system, IP telephones that are in the TTI state are unregistered.

   To verify if the TTI for voice terminals option is turned on:

   a. Type `display system-parameters features`. Press `Enter`.

      The system displays the Feature-Related System Parameters screen.

   b. Press `Next` until you see the **TTI/PSA Parameters** section.

   c. Ensure that the **Terminal Translation Initialization (TTI) Enabled?** field is set to y.

   d. Ensure that the **TTI State** field is set to voice.

   e. Press `Enter`.

      Important:

      Administrators or technicians might often turn off TTI during software upgrades. Remember that you must turn TTI back on when the upgrade is complete.

      Security alert:

      You might choose to leave TTI turned off for security reasons. If you want to use the feature but not use TTI, set the **TTI FAC** field on the Feature Access Code (FAC) screen to blank.

Enabling unnamed registration for IP endpoints

Procedure

1. Type `display system-parameters customer options`. Press `Enter`.

   The system displays the Optional Features screen.
2. On the Optional Features screen, click **go to page** and type `5` to view the **Personal Station Access (PSA)** and the **Terminal Trans. Init. (TTI)** fields.
3. Ensure that the **Personal Station Access (PSA)** field is set to `y`.
4. Ensure that the **Terminal Trans. Init. (TTI)** field is set to `y`. If **Personal Station Access (PSA)** and **Terminal Trans. Init. (TTI)** show `n`, go to the SMI Feature Administration page and click **ON**.
5. To exit the screen, click the **cancel** tab.
6. Type `change system-parameters feature`. Press `Enter`.

   The system displays the Feature-Related System Parameters screen.
7. On the Feature-Related System Parameters screen, click **go to page** and type `3` to gain access to the **Terminal Translation Initialization (TTI) Enabled** field.
8. Set the **Terminal Translation Initialization (TTI) Enabled** field to `y`.
9. Set the **TTI state** field to `voice`.
10. Set the **Default COR for Dissociated Sets** field to a valid COR number.
11. Set the **Unnamed Registration and PSA for IP Telephones** field to `y`.
12. To save the changes, click the **enter** tab.
13. Type `change system-parameters security`. Press `Enter`.

    The system displays the Security-Related System Parameters screen.
14. On the Security-Related System Parameters screen, click **go to page** and type `2` to gain access to the **Receive Unencrypted from IP Endpoints** field.
15. Set the **Receive Unencrypted from IP Endpoints** field to `y`.
16. To save the changes, click the **enter** tab.
17. Type `change ip-network-map`. Press `Enter`.

    The system displays the IP Address Mapping screen.
18. In the **IP Address Range** field, specify a range of IP addresses for the set of IP endpoints within the network.
19. In the **Subnet** field, specify the subnet mask.
20. In the **Network Region** field, specify a network region number.
21. To save the changes, click the **enter** tab.

Screens for administering Emergency Calls from Unnamed IP Endpoints

Screen name	Purpose	Fields
Optional Feature	Ensure that the feature description and implementation feature is enabled on the system.	• G3 Version • Personal Station Access (PSA) • Terminal Trans. Init. (TTI)
Feature-Related System Parameters	Ensure that the Emergency Calls from Unnamed IP Endpoints feature is enabled on your system.	• TTI/PSA Parameters • Terminal Translation Initialization (TTI) Enabled? • TTI State • Default COR for Dissociated Sets • Unnamed Registration field
Security-Related System Parameters	User can merge IP phones to TTI service or separate IP phones from TTI service using the respective FAC.	• IP Stations in TTI State
IP Address Mapping	System Admin defines the range of IP addresses for the set of IP endpoints within the network. Each range of IP address is mapped to specific Network region.	• IP Address Range • Subnet • Network Region

Reports for Emergency Calls from Unnamed IP Endpoints

The following reports provide information about the Emergency Calls from Unnamed IP Endpoints capability:

- Call Detail Recording (CDR)

  If an IP telephone that is in TTI service makes an outgoing call, CDR records contain the port as the calling party. An example of a port is S00001.

- History Log

  If the **Record IP Registrations in History Log?** field on the System-Parameters Features screen is set to y, the system records registrations to TTI service and unregistrations from TTI service in the History Log. The History Log displays the:

  - IP address for registrations and unregistrations

  - Telephone extension for Personal Station Access (PSA) associations and PSA disassociations

    The same information is available from the Tracelog file. The Qualifier column shows the IP address. The system also records state changes to and from TTI service from LoginInfoUpdate messages, end user PSA, or similar actions.

- The List Usage Report lists IP telephones that are in TTI service. To see the List Usage Report report, type the `list usage ip-address n`, where *n* is the IP address of the telephone.
- Tracelog

  Registrations to, and unregistrations from, TTI service get an entry in the tracelog file, if the Linux Registries has turned on each system for the appropriate platforms. Extensions that move from one telephone to another also get an entry in the tracelog file.
- The TTI Service IP Stations report lists IP telephones that are in TTI service. To see the TTI Service IP Stations report, type the **`list tti-ip-stations`** command.

For more information on these reports and the associated commands, see *Avaya Aura® Communication Manager Reports*.

Interactions for Emergency Calls from Unnamed IP Endpoints

This section provides information about how the Emergency Calls from Unnamed IP Endpoints feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Emergency Calls from Unnamed IP Endpoints in any feature configuration.

E911 restricted telephones

You might have telephones from which you do not want users to make or receive external calls. You can put such telephones into TTI service. However, an improved method is to give the telephone an extension number, and then use a Class of Restriction (COR) to restrict the permissions.

For example, if someone dialed 911 from such a telephone and the call accidentally dropped, the public safety officer will call back to the calling party number that the public safety office received during the 911 call. If the telephone that dialed 911 has an extension number, the telephone receives the return call. If the telephone that dialed 911 was in TTI service, the return call rings someone else who does not know about the emergency.

Selective Conference Party

With the Selective Conference Party feature, a member of a conference call can view the number and the name of the other parties on the call. The member can also drop or mute the other parties. A telephone that is in TTI service cannot use the Selective Conference Party feature because the

feature requires the use of a button. However, a telephone that is in TTI service can be displayed, dropped, or muted.

Chapter 78: Emergency call routing for H.323 visiting users

With this feature, Communication Manager receives emergency SIP trunk calls made by H.323 visiting users.

For example, a user from Location A is travelling on business to Location B. Location A and Location B can be controlled by the same Communication Manager or different Communication Manager managed by a single System Manager. An emergency call made by the user at Location B routes to the nearest possible PSAP agency in Location B even if the user dials the emergency number of Location A. Depending upon the station configuration, the CPN can be the station extension or ELIN of the user. The attendant endpoints at Location B display the calling party number (CPN) as the identity of the user. PSAP receives the CPN that is sent over a PSTN trunk as the identity of the user.

If an emergency call disconnects, PSAP calls back the CPN. Communication Manager forwards the call to the phone that made the emergency call. In the **Emergency Extension Forwarding (min)** field, you can set the time in minutes for the trunk to forward the call to the extension that made the emergency call. This field is available on the Feature-related system parameters screen.

Screens for administering Emergency call routing for H.323 visiting users

Screen name	Purpose	Fields
Signaling Group	To enable crisis alert incoming SIP trunk call.	Alert Incoming SIP Crisis Calls
Special Applications	To enable crisis alert only at the location of the caller.	(SA9065) - Crisis Alert to Stations by Location
Feature-Related System Parameters	To enable crisis alert across tenant partitions.	Allow crisis alert across tenants

Table continues…

Screen name	Purpose	Fields
Feature-Related System Parameters	To set the time in minutes for the trunk to forward the call to the extension that made the emergency call.	Emergency Extension Forwarding (min)
Stations	To override ELIN with the station extension.	Always use

Note:

When you enable the **(SA9065) - Crisis Alert to Stations by Location** field, only the attendant endpoints and stations configured with **crss-alert** button at Location B are notified about the emergency call.

When you enable the **Allow crisis alert across tenants** field, the attendant endpoints across all tenant partitions are notified about the emergency call.

Administering crisis alert of Emergency call routing for H.323 visiting users

Procedure

1. Type `change signaling group`.
2. Set the value of **Alert Incoming SIP Crisis Calls** to `y`.

   Note:

   The **Alert Incoming SIP Crisis Calls** field is available only for the SIP group type.
3. Save the changes.

Chapter 79: Enbloc Dialing and Call Type Digit Analysis

Using the Enbloc Dialing and Call Type Digit Analysis feature, users can automatically place outgoing calls based on the telephone number information in the telephone's call log, without the user having to modify the telephone number.

For more information, see *Avaya Aura® Communication Manager Screen Reference*.

Detailed description of Enbloc Dialing and Call Type Digit Analysis

With the Call Type Digit Analysis feature, you can specify how Communication Manager must modify a telephone number to route a call when the call is made using:

- Call logs
- Contacts
- A corporate directory

When the telephone number in call log, contacts, or a corporate directory is not in a routable format, Communication Manager performs the digit analysis without matching the number with the Dial Plan Analysis screen. For example, the number (212) 848-2249 cannot be routed directly. The number must be dialed as (91212) 848-2249. To convert the number to a routable format, you must enable one of the following options:

- The endpoint to modify the number.
- Communication Manager to modify the number using the Call Type Digit Analysis feature.

The Call Type Digit Analysis feature is available with Communication Manager Release 4.0 or later. 96xx and 96x1 H.323 IP telephones, Avaya one-X® Communicator H.323 soft clients, and Avaya one-X® Mobile Edition for S60 Dual Mode SIP endpoints support this feature. These endpoints activate Call Type Digit Analysis using a signal while sending the contents of a call log entry.

With the Call Type Digit Analysis feature in Communication Manager Release 7.0 or later, the system can:

- Process the plus sign (+) in the missed or answered call log of an H.323 endpoint.
- Perform location-based digit conversion on numbers dialed from an endpoint.

When Communication Manager finds a match for the dialed string on the Call Type Digit Analysis table, Communication Manager :

1. Deletes and inserts the digits according to the first priority administered for the string in the table.
2. Tests the modified digit string with the following administered call types: ext, udp, aar, and ars.
   - If the modified digit string matches with an administered call type, Communication Manager routes the call.
   - If the modified digit string does not match with an administered call type, Communication Manager processes the digits according to the next priority administered for the string. Communication Manager tests the modified digit string with the administered call types.
3. Routes the call using the original unmodified digits and the dial plan if a match is not found for the dialed string.

Enbloc Dialing recovery strategy and behavior

During server recovery, Enbloc dialing maintains full or partial functionality, depending on the type of server recovery.

Enbloc works as designed when the following servers are in local survival mode:

- Server duplication
- Survivable Remote Server
- ATM WAN Spare Processor
- SREPN
- Survivable Core Server

Call-type high-level capacities

Communication Manager provides four manipulations and call-type choices per Call Type Digit Analysis entry.

- Digit manipulations and call-type choices = groups of Del, Insert, Type, corresponding to the various ways one might need to interpret a single digit string to make it something routable.

See *Avaya Aura® Communication Manager System Capacities Table* under Documentation on http://support.avaya.com for additional capacities information.

Enbloc Dialing and Call Type Digit Analysis administration

The following task is part of the Enbloc Dialing and Call Type Digit Analysis feature:

- Administering Call Type Digit Analysis

Related links

Administering Call Type Digit Analysis on page 673
Example of Call Type Digit Analysis on page 673

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.

Example of Call Type Digit Analysis

The example shows an administered Call Type Digit Analysis Table.

```
display calltype analysis                                          Page 1 of x
                        CALL TYPE DIGIT ANALYSIS TABLE
                                    Location:   all
    Dialed String             Delete Insert     Type    Delete Insert       Type
Match: 303_______________ 1: 0      __________ ars  2: 0__    1__________ ars
length: Min 10 Max 10    __ 3: 3      __________ ext  4: 0      011_______ ars
```

In the 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.

End User Procedures for Enbloc Dialing and Call Type Digit Analysis

To allow Communication Manager to use **Enbloc Dialing and Call Type Digit Analysis**, a user must place a call from call log or corporate directory. However, if the user places the call by dialing digits on keypad, Communication Manager uses **Dial Plan** to route the call.

Interactions for Enbloc Dialing and Call Type Digit Analysis

This section provides information about how the Enbloc Dialing and Call Type Digit Analysis feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Enbloc Dialing and Call Type Digit Analysis in any feature configuration.

Call Detail Recording (CDR)

In the custom CDR record for each call, a data element records whether or not Call Type Digit Analysis was used for the call.

Call Management System (CMS)

CMS receives the unmodified digit string as sent by the phone to Communication Manager.

Extended Trunk Access (ETA)

ETA node number manipulation takes place only after Enbloc Dialing fails to match the dialed string against the Call Type Analysis Table, and the call is routed to the Communication Manager dial plan.

Integrated Management (IM)

IM provides access to the Call Type Digit Analysis Table.

Personal Central Office Line (PCOL)

A call routed over a PCOL trunk does not receive Call Type Digit Analysis.

Chapter 80: Encrypted SRTCP

Use the Encrypted SRTCP feature to provide enhanced security for the media control streams associated with the RTP media stream.

Note:

The RTP and RTCP streams are two consecutive UDP ports. The RTCP control stream conveys usage data. An example of usage data is the identification of the two parties on a given call.

Detailed description

With the Encrypted SRTCP feature, you can protect media control streams. To support this feature, the **Encrypted SRTCP** field is available on the ip-codec-set SAT screen. The following are the available policy modes:

- Force Encrypted SRTCP: To permit only encrypted SRTCP calls and to achieve high security standards. If you set the field to `enforce-enc-srtcp`, all the crypto profiles enforce encrypted SRTCP.
- Best Effort: To facilitate negotiation of the encrypted SRTCP parameter. If you set the field to `best-effort`, Communication Manager facilitates negotiation of Encrypted SRTCP capability between the endpoints. All endpoints must support negotiation to enforce the Best Effort policy mode.
- Force Unencrypted SRTCP: To support backward compatibility. If you set the field to `enforce-unenc-srtcp`, all the crypto profiles enforce unencrypted SRTCP.

Screen for administering Encrypted SRTCP

Screen name	Purpose	Fields
Ip-codec-set	To select a policy option to activate the encrypted SRTCP.	Encrypted SRTCP

Administering Encrypted SRTCP

Before you begin

Ensure that the **Media Encryption Over IP?** field on the system-parameters customer-options screen is set to `y`.

Procedure

1. On the SAT screen, type `change ip-codec-set n`, where n is the number corresponding to the codec set that you want to change.
2. In the **Encrypted SRTCP** field, type `enforce-enc-srtcp`. You can select the **Best Effort** option if you want Communication Manager to negotiate encrypted SRTCP capability between endpoints.

   Note:

   The default value for Encrypted SRTCP is `enforce-unenc-srtcp`. Endpoints earlier than Release 7.0 do not support encrypted SRTCP. Therefore, enforcing unencrypted SRTCP is preferable in networks that have Communication Manager Release 7.0 with earlier endpoints.
3. Save and exit.

Interactions for Encrypted SRTCP

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

Emergency calling

Using the encryption options, you cannot negotiate calls with the destination party because of protocol incompatibilities. The protocol incompatibility results in the inability to pass certain types of emergency calls. Therefore, you must configure the network to ensure best routing of calls.

Media Encryption using AES

If the RTP media encryption is set to none, the enforce-encrypted SRTCP rules do not apply to the RTP/RTCP streams.

Chapter 81: End-to-end secure call indication

With the End-to-end secure call indication feature, a SIP phone displays an icon indicating the security of a SIP call. The displayed icon is similar to the icon displayed by a web browser when a user visits a secured website.

Detailed description of End-to-end secure call indication

With the End-to-end secure call indication feature, a SIP phone displays the security icon  , indicating the security of a SIP call.

The SIP phone displays the security icon when the end-to end call has the following setup:

- Media is SRTP.
- SIP signaling is TLS.
- Media Server signaling links or Media Gateway links, if applicable, are TLS.

The security levels of SIP signaling coming from Session Manager are based on the Av-header.

The End-to-end secure call indication feature is applicable only for point-to-point calls. The icon on the SIP phone displays the call as secured only for two-party calls. However, when a third-party is involved, such as a conference, the icon displays the call as unsecured even if the call is on a secured network.

Session Manager uses a new header called Av-Secure-Indication to convey the end-to-end security of the call. For information about:

- Overview of the End-to-end secure call indication feature on Session Manager, see *Avaya Aura® Session Manager Overview and Specification*.
- Configuring the End-to-end secure call indication feature on Session Manager, see *Administering Avaya Aura® Session Manager*.
- Capacity information, see:
  - *Avaya Aura® Session Manager Overview and Specification*
  - *Deploying Avaya Aura® Session Manager*

Screen for administering End-to-end secure call indication

Screen name	Purpose	Fields
Signaling group	To enable the End-to-end secure call indication feature.	• **Enabled Layer 3 Test** • **Peer Detection Enable**

Administering End-to-end secure call indication

Procedure

1. On the SIP Signaling Group screen, set the following fields to `y`:
   a. **Enabled Layer 3 Test**
   b. **Peer Detection Enabled**

      Communication Manager automatically detects the peer server.
2. If the peer server is not Session Manager, set the **Peer Server** field on the SIP Signaling Group screen to Session Manager.

   If the peer server is Session Manager, Session Manager inserts a +av.sci parameter in the OPTIONS response. Based on the presence of the +av.sci parameter, Communication Manager identifies the peer server as secured. If the OPTIONS response from Session Manager does not contain the secured call indication, the SIP element considers the request as unsecured. The SIP element inserts or overwrites the Av-Secure-Indication header with the value unsecured in the message.

Chapter 82: Support for Enhanced Access Security Gateway

Communication Manager supports Enhanced Access Security Gateway (EASG). EASG is a certificate based challenge-response authentication and authorization solution. Avaya uses EASG to securely access customer systems and provides support and troubleshooting.

EASG provides a secure method for Avaya services personnel to access the Communication Manager remotely and onsite. Access is under the control of the customer and can be enabled or disabled 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 Health check. EASG must be enabled for Avaya Services to perform the required maintenance tasks.

You can enable or disable EASG through Communication Manager.

EASG only supports Avaya services logins, such as init, inads, and craft.

Discontinuance of ASG and ASG-enabled logins

EASG in Communication Manager 7.1.1 and later replaces Avaya's older ASG feature. In the older ASG, Communication Manager allowed the creation of ASG-enabled user logins through the SMI Administrator Accounts web page. Such logins are no longer supported in Communication Manager 7.1.1 and later. When upgrading to Communication Manager 7.1.1 or later from older releases, Communication Manager does not support ASG-enabled logins.

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

Enabling or disabling EASG through the CLI interface

About this task

Avaya recommends enabling EASG. By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (http://support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.

Procedure

1. Log in to the Communication Manager CLI interface as an administrator.
2. To check the status of EASG, run the following command: `EASGStatus`.
3. To enable EASG (Recommended), run the following command: `EASGManage --enableEASG`.
4. To disable EASG, run the following command: `EASGManage --disableEASG`.

Enabling or disabling EASG through the SMI interface

About this task

By enabling Avaya Services Logins you are granting Avaya access to your system. This setting is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. The product must be registered using the Avaya Global Registration Tool (GRT) at https://grt.avaya.com for Avaya remote connectivity. See the Avaya support site support.avaya.com/registration for additional information for registering products and establishing remote access and alarming.

By disabling Avaya Services Logins you are denying Avaya access to your system. This setting is not recommended, as it can impact Avaya's ability to provide support for the product. Unless the customer can manage the product, Avaya Services Logins should not be disabled.

Procedure

1. Log on to the Communication Manager SMI interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the **Security** section, click **Server Access**.
4. In the **Avaya Services Access via EASG** field, select:
   - **Enable** to enable EASG.
   - **Disable** to disable EASG.
5. Click **Submit**.

Viewing the EASG certificate information

About this task

Use this procedure to view information about the product certificate, which includes information about when the certificate expires.

Procedure

1. Log in to the Communication Manager CLI interface.
2. Run the following command: `EASGProductCert --certInfo`.

EASG product certificate expiration

Communication Manager raises an alarm if the EASG product certificate has expired or is about to expire in 365 days, 180 days, or 30 days. To resolve this alarm, the customer must apply the patch for a new certificate or upgrade to the latest release. Else, the customer loses the ability for Avaya to provide remote access support.

If the EASG product certificate expires, EASG access is still possible through the installation of EASG site certificate.

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge or response.

Managing site certificates

Before you begin

1. Obtain the site certificate from the Avaya support technician.
2. You must load this site certificate on each server the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to /home/*cust* directory, where *cust* is the login ID. The directory might vary depending on the file transfer tool used.
3. Note the location of this certificate and use in place of *installed_pkcs7_name* in the commands.

4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

Procedure

1. Log in to the CLI interface as an administrator.
2. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
3. To view information about a particular certificate, run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.
4. To delete the site certificate, run the following command:
   - `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   - `sudo EASGSiteCertManage --delete all`: To delete all the site certificates currently installed on the system.

Chapter 83: Enhanced 911

Use the Enhanced 911 (E911) feature to quickly access your local public safety agency. The public safety agency can dispatch the appropriate response team in cases of a:

- Fire
- Accident
- Crime
- Medical emergency

Detailed description of Enhanced 911

A caller who needs emergency assistance dials one of the following Universal Emergency Numbers (UENs):

- 911 in the United States
- 000 in Australia
- 112 in the European community

The system routes the call through a local central office (CO), through an emergency tandem office, to the appropriate public safety answer point (PSAP). The PSAP answers the call.

A tandem office can route the call to a PSAP in surrounding areas. In the United States, a tandem office can route the call to nearby area codes. If the PSAP that receives the call is the incorrect PSAP to handle the emergency, the PSAP transfers the call to the correct PSAP. Transfers can only occur between geographically adjacent or nearby PSAPs.

Each PSAP usually covers one city, or one rural county or community. At the PSAP, emergency operators determine the nature of the emergency, and contact the appropriate response agency. In the United States, a PSAP is usually responsible for an area that covers several independent police and fire departments.

With E911, the system sends the call and the Calling Party Number (CPN) over Centralized Automatic Message Accounting (CAMA) trunks. The system can also send the call and the CPN through the calling number information element (IE) over Integrated Services Digital Network (ISDN) trunks.

To learn how CAMA and ISDN trunks translate an extension to the PSAP, see *Administering Avaya Aura® Communication Manager*.

The public emergency system maintains a database that stores location and background information to help public safety agencies respond quickly with the appropriate assistance. The PSAP uses the CPN or the Caller Emergency Service Identification (CESID) number to look up the street address of the caller. The PSAP uses an Automatic Location Information (ALI) database. The ALI database is usually owned and managed by local exchange carriers (LEC). Instead of a LEC, customers can also contract with a third party to update the ALI database for them.

The E911 feature does not provide PSAP with the location of the person who placed the emergency call if the call came from a telephone that is on:

- A system that is not equipped with CAMA, ISDN trunks, or SIP trunks
- An adjunct computer system that is associated with CAMA, ISDN trunks, or SIP trunks

Instead, the E911 system identifies only the location of the trunk termination.

To solve this problem, you can report the emergency location extension as the CPN. After someone moves a telephone, you can manually correlate the CPN with the new telephone location. You can also purchase an adjunct that performs this correlation and update for you. You do not have to update the ALI database for the public switched telephone network (PSTN) after each telephone move.

The E911 feature transmits the extension of a direct inward dialing (DID) telephone that is associated with the calling party. The E911 feature transmits either:

- CESID over CAMA trunks
- CPN over ISDN trunks

The calling party might be at or near a telephone on a remote port network. The calling party might also be at a remote location that is served by an off-premises telephone.

Important:

If you use the digit 9 on the Dialplan Analysis Table screen as the ARS access code, also administer the dial string 11 as either an emer or alrt number. That way, when a user dials 911, the digit 9 provides an outside line, and the digits 11 indicate an emergency or crisis alert call.

For Avaya IP Softphone, if the **Remote Softphone Emergency Calls** field on the Station screen is set to as-on-local, the system processes information based on certain criteria. For more information on what the system does when the **Remote Softphone Emergency Calls** field is set to as-on-local, see *Administering Avaya Aura® Communication Manager*.

E911 configurations with gateways in different locations

Gateways in different locations might have a different PSAP than the PSAP of the main server. You must ensure that the system correctly routes emergency calls that are made from telephones that are registered to each gateway to the correct PSAP.

To ensure that a gateway in a separate location can route emergency calls properly, the system requires a CO trunk, a CAMA trunk, or a Primary Rate Interface (PRI) trunk from the gateway to the LEC. You must administer each gateway that is in a different PSAP jurisdiction than the main server in a separate location. This separate administration ensures that the system can route

emergency calls from that location. If a gateway is in the same PSAP jurisdiction as the main server, you do not need to administer the gateway in a separate location.

E911 location Specific Routing

In a configuration with one location, the system routes all outgoing calls to the PSTN according to the Automatic Route Selection (ARS) table for location 1. If gateways are in different locations, you must administer Location Specific Routing for each location.

If a gateway is in a separate location from the main server, you can administer the gateway in locations for Linux and Avaya DEFINITY servers. For more information, see the *Avaya Aura® Communication Manager System Capacities Table*.

The command for Location Specific Routing is **change ars analysis location** *X 0*, where *X* is the chosen location (2 to 64 or 2 to 44), and *0* is the first placeholder in the analysis table. Once the system displays the table, enter the routing information:

- Chosen dialed string (for example, 911)
- Minimum and maximum number of digits
- Route pattern
- Call type

You must also set up the required route pattern information. When you complete this administration, the system routes emergency calls from the location over a CO trunk, a CAMA trunk, or a PRI trunk to the LEC.

1. If a gateway is connected to the LEC over a CO trunk, the extension of the CO trunk identifies the gateway service address. The service address is the physical location that the PSAP sees. Calls from any telephone that is registered to the gateway display the CO trunk extension to the PSAP. The PSAP then sends the emergency response to the service address.

   Use the CO trunk to send and receive emergency calls only. You must verify with the LEC that the extension of the CO trunk is in the PSAP database so that all emergency help is sent to the correct location.

2. If a gateway is connected to the LEC over a PRI trunk, the system sends an extension to the PSAP based upon how Communication Manager is administered. You must verify with the LEC that all the extensions are in the PSAP database. For more information, see *Administering Avaya Aura® Communication Manager*.

3. If you use DID numbers from the main server to administer the extensions at the gateway, the numbers that are used at the gateway must be moved to the CO where the 911 calls terminate. If the numbers are not moved, emergency help is sent to the main server location and not to the gateway location.

If the main server and the gateway are in different LEC jurisdictions:

- If you use a CO trunk from the gateway to the central office, follow the procedure as previously described in Step 1. Ensure that the correct extension is in the PSAP database for the CO trunk. All calls that are made from the gateway use this extension. Also ensure that

the correct street address is in the PSAP database for the CO trunk. All calls that are made from the gateway use this street address.

- If you use a PRI trunk, you can purchase a block of DID extensions from the LEC for your gateway telephones. You can shorten the gateway extensions for private calls within your system. For example, you can shorten extension 765-4321 to 4321.

  When the system calls the PSTN, you must use the complete extension so that the number is recognized at the PSAP. For example, the system must send extension 765-4321 to the PSAP. The PSAP does not recognize extension 4321. Some PSAPs require a 10-digit number.

These two scenarios apply to each gateway that is in a separate location. You must repeat each applicable procedure for each gateway that is connected to a server with a unique PSAP. You must also repeat this procedure for each gateway that is in its own location.

You can use the same Location Specific Routing tables and trunks for:

- Gateways that are in the same location as the main system
- Multiple gateways that are in the same location

Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to the Enhanced 911 feature.

E911 for wired IP telephones

Important:

When someone dials an emergency number from an Avaya IP telephone, the emergency call reaches the local emergency service in the PSAP only when the telephone system has local trunks. If someone dials an emergency number from a remote location that does not have local trunks, an Avaya IP telephone cannot dial to and connect with local emergency services. To avoid possible delays in getting emergency aid, do not use an Avaya IP telephone to dial emergency numbers from a remote location. Avaya is not responsible or liable for any damages that might result from misplaced emergency calls that someone makes from an Avaya IP telephone. Your use of Communication Manager indicates that you have read this advisory. You further agree to use an alternative telephone to dial all emergency calls from remote locations. If you have questions about emergency calls from an IP telephone, go to the Avaya Support website at http://support.avaya.com for related documentation and knowledge articles .

When someone dials an emergency number from a wired IP telephone, the system assigns an Emergency Location Information Number (ELIN) through an IP subnetwork. The system then sends the ELIN over either CAMA or ISDN PRI trunks to the emergency services network. To use this capability, you must have subnetworks that correspond to geographical areas.

The E911 for wired IP telephones capability works with two types of IP protocols:

- H.323
- SIP

If someone dials an emergency number from a wired IP telephone, the system at the PSAP uses the CPN to look up the physical location of the caller. However, the CPN might not always correspond to the physical location of the caller, because users with:

- H.323 IP telephones can move the telephones without notifying the system administrator
- SIP IP telephones can use the same extension simultaneously at several different telephones

Without the E911 for wired IP telephones capability, the emergency response personnel might go to the wrong physical location. With the E911 for wired IP telephones capability, the system properly identifies the location of the caller. The emergency response personnel can go to the correct physical location, even if an emergency call comes from a bridged call appearance.

When someone uses an IP telephone to dial an emergency number, the software compares the following two values for that IP telephone:

- The **Emergency Location Extension** field on the IP Address Mapping screen
- The **Emergency Location Ext** field on the Station screen
  - If the two values are the same, the telephone most likely did not move. If the telephone did move, the telephone moved within the same subnetwork. In this scenario, Communication Manager sends the station's own extension as the Calling Party Number (CPN) .
  - If the two values are different, and if the Emergency Location Extension on the IP Address Mapping screen is not blank, the telephone moved from one subnetwork to another. In this scenario, Communication Manager sends the CPN that is on the IP Address Mapping screen.
  - If the Emergency Location Extension on the IP Address Mapping screen is blank, the administrator expects the caller to be located outside the LAN. This situation is true for a softphone. In this scenario, the CPN sent by Communication Manager is the Emergency Location Extension on the Station screen.

Whenever you add an extension as an Emergency Location Extension to the IP Address Mapping screen, check all Station screens for telephones in that IP address range.

- If the telephone is a DID number, ensure that the Emergency Location Extension is the same on both the Station screen and the IP Address Mapping screen.
- If the telephone is not a DID number, ensure that the Emergency Location Extension on the Station screen is different from the Emergency Location Extension on the IP Address Mapping screen.

Emergency Extension Forwarding

If an emergency call is dropped, the public safety personnel immediately attempt to call back. If the ELIN that was sent is not equivalent to the extension number of the caller, the return call rings at a different telephone. To overcome this situation, you can, for an administered period of time, automatically forward all calls to the telephone that placed the emergency call.

Use the **Emergency Extension Forwarding (min)** field on the Feature-Related System Parameters screen to set the Emergency Extension Forwarding timer for all incoming trunk calls if an emergency call is dropped.

This Emergency Extension Forwarding applies only if the Emergency Location Extension is an extension on the same system as the extension from which 911 was dialed. Customers who have several systems in a campus should assign several emergency location extensions.

Call Forwarding of dropped emergency calls scenario

In this scenario, an IP telephone and a nearby gateway that provides a connection to the PSTN are both registered to a primary server. The gateway is backed up by a Survivable Remote Server, and the IP telephone has some Survivable Remote Servers in its alternate gatekeeper list. The IP telephone dials 911, and then the LAN shuts down abnormally and recovers partially.

If both the IP telephone and the gateway can reregister to the primary server, no problem exists. Also, if both the IP telephone and the gateway are forced to register with the same Survivable Remote Server, no problem exists.

However, if the IP telephone or the gateway re-registers to a Survivable Remote Server and the other re-registers to the primary server, or if the IP telephone and the gateway re-register to different Survivable Remote Servers, a minor problem exists.

When the emergency response personnel call back, the server that the gateway is registered with determines that the IP telephone is unregistered. The server cannot forward the return call to the IP telephone. Instead, the server attempts to forward the call to a telephone that is equivalent to the sent ELIN.

Even with automatic Emergency Return Call Forwarding, select the Emergency Location Extension that is administered in the ip-network-map screen as follows:

- On gateways that have incoming PSTN trunks
- On the same gateway as the telephones that the gateway covers, assuming that the gateway has incoming PSTN trunks

Crisis Alert for emergency calls

The Crisis Alert capability notifies the attendant, up to 10 other designated users, or a digital pager when someone dials an emergency number. Designated users might include:

- Security guards
- Receptionists
- Secretaries
- Front office personnel
- Human resources personnel

If a person dials an emergency number, the attendant or other designated users might want to know who made the call so that they can direct the emergency personnel to the right place.

When a user dials an emergency number, the system sends both an audible alert and a visual alert to the attendant console and the telephone of the designated user.

- The audible alert is a siren alarm.

- The visual alert is a flashing **crss-alert** button. The system also displays the name and the extension of the caller.

  If a user, John Doe at extension 3041, dialed an emergency number, the screen of attendant consoles and digital telephones with a **crss-alert** button display the following information:

  EM=JOHN DOE 3041 EM

Crisis Alert cancellation

To cancel the alert, you can administer the system so that only one notified user must acknowledge the alert, or all notified users must acknowledge the alert.

To cancel an emergency alert, an attendant must press the **crss-alert** button on the attendant console three times:

- The first press turns off the siren alarm.
- The second press stops the crss-alert lamp from flashing.
- The third press clears the display.

Digital telephone users must press the **crss-alert** button on the telephone to cancel the emergency alert.

- If only one user must acknowledge the alarm, the siren alarm stops and the display gets cleared at all telephones.
- If all administered users must acknowledge the alarm, the alarm continues at each telephone until the user of that telephone presses the **crss-alert** button. Once all administered users acknowledge the alarm, the siren alarm stops. The name and the extension of the person who dialed the emergency number remains on the telephone display. To completely cancel an alert and clear the display, each administered user must press the **normal** button.

If someone makes an emergency call while another crisis alert is still active, the second emergency call is placed in a queue. If you administer the system so that:

- All users must acknowledge the alert, all users must acknowledge all emergency calls. The calls might not appear in the queue in the order that the calls were made.
- Only one user must acknowledge the alert, the first alert remains active at the telephone from where the alert was acknowledged. Any subsequent calls are queued to the next available telephone, in the order that the calls were made.

Once you administer the Crisis Alert capability, the system continues to record each emergency call. The system also sends a record to the system printer, if a system printer is available. If a system printer is not available, you can type `list emergency` to view the Emergency Access Calls report.

Enhanced 911 administration

The following steps are part of the administration process for the Enhanced 911 feature:

- Setting up Crisis Alert to an attendant or a display telephone
- Setting up Crisis Alert to notify a digital pager
- Setting up emergency extension forwarding
- CAMA numbering administration for Enhanced 911

Related links

Setting up Crisis Alert to an attendant or a display telephone on page 692
Setting up Crisis Alert to notify a digital pager on page 694
Setting up emergency extension forwarding on page 695
CAMA numbering administration for Enhanced 911 on page 696

Preparing to administer Enhanced 911

Procedure

1. Set up calling party restrictions on the Class of Restriction screen.

   For information on how to set up a Class of Restriction (COR), see the Class of Restriction feature.

2. Set up ARS access codes on the Feature Access Code (FAC) screen.

   For information on how to set up a FAC, see the Feature Access Code feature.

3. Set up all telephone route patterns on the Route Pattern screen.

   For information on how to set up a route pattern, see the Uniform Dial Plan feature.

Screens for administering Enhanced 911

Screen name	Purpose	Fields
ARS Digit Analysis Table	Set up an emergency number that users dial to access emergency services.	All
Attendant Console	Notify the attendant when someone dials the emergency number.	Any available button field in the **Feature Button Assignments** area.
CAMA Numbering - E911 Format	Format CAMA trunks for dialing.	All
Class of Restriction	Ensure that calling party restrictions are set up on your system.	Calling Party Restriction

Table continues…

Screen name	Purpose	Fields
Crisis Alert System Parameters	Force all users who have a **crss-alert** button on the telephone to acknowledge a crisis alert.	Every User Responds
	Administer the Crisis Alert capability to send an alert to a digital pager.	All fields in the **Alert Pager** area
Feature Access Code (FAC)	Ensure that FACs for ARS access codes are set up on your system.	• ARS Access Code 1 • ARS Access Code 2
Feature-Related System Parameters	Set the timer to forward all incoming trunk calls in an emergency.	Emergency Extension Forwarding (min)
Optional Features	Ensure that your system is set up to handle Automatic Route Selection (ARS) routing and digit analysis.	ARS
Route Pattern	Ensure that you have set up route patterns on your system.	All
Station	Notify another user when someone dials the emergency number.	Any available button field in the **Button Assignments** area.
	Determine when to use the extension as E911 CPN.	• Remote Softphone Emergency Calls • Emergency Location Ext • Always Use

Setting up Crisis Alert to an attendant or a display telephone

Procedure

1. Set up the emergency number
2. Set up the attendant console to receive emergency notification
3. Set up digital telephones to receive emergency notification
4. Set which users must acknowledge the emergency alert

Setting up the emergency number

Before you begin

On the Optional Features screen, ensure that the **ARS** field is set to y.

If this field is set to n, your system is not set up for the Enhanced 911 feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering emergency numbers, or to open a service request.

To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

Procedure

1. Type `change ars analysis n`, where *n* is the number of the ARS table that you want to change. Press `Enter`.

   The system displays the ARS Digit Analysis Table screen.
2. In the **Dialed String** field, type the number that users dial to reach emergency services.
3. In the **Total Min** and **Total Max** fields, type the number of digits that you typed in the **Dialed String** field.

   The user must dial all 3 digits in the **Dialed String** field for the system to treat the call as an emergency call.
4. In the **Route Pattern** field, type the number of the route pattern for local calls.
5. In the **Call Type** field, type `emer` or `alrt`.
   - emer identifies the number in the **Dialed String** field as an emergency call.
   - alrt ensures that the number in the **Dialed String** field activates emergency alert notification.
6. Press `Enter` to save your changes.

Setting up the attendant console to receive emergency notification

About this task

When Crisis Alerting is active at the attendant console, the console is in position-busy mode. No other incoming calls interfere with the emergency call, but the console can still originate calls. The attendant must press the **position-busy** button to unbusy the console. The attendant must then press the **crss-alert** button to deactivate the audible and the visual alerts.

Procedure

1. Type `change attendant n`, where *n* is the number of the attendant console. Press `Enter`.
2. On the Attendant Console screen, click **Next** until you see the **Feature Button Assignments** area.
3. In the **Feature Button Assignments** area, assign crss-alert to a button.
4. Press `Enter` to save your changes.

Setting up digital telephones to receive emergency notification

Before you begin

- On the Station screen for each telephone that you want to receive emergency notification:
  1. Ensure that the extension is a digital display telephone.
  2. In the **Type** field, ensure that the telephone is not a virtual extension.

  To view the Station screen, type `change station n`, where *n* is the extension. Press `Enter`.

Procedure

1. Type `change station n`, where *n* is the extension of the security guard. Press `Enter`.
2. On the Station screen, click **Next** until you see the **Button Assignments** area.
3. In the **Button Assignments** area, assign crss-alert to an available button.

   Note:

   You cannot assign the crss-alert button to a softkey.
4. Press `Enter` to save your changes.

   you can repeat this process for the telephone of each security guard.

Setting which users must acknowledge the emergency alert

Procedure

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

   The system displays the Crisis Alert System Parameters screen.
2. In the **Every User Responds** field, type `y`.

   If you set the **Every User Responds** field to n, any one of the designated users can cancel an alert.
3. Press `Enter` to save your changes.

Setting up Crisis Alert to notify a digital pager

About this task

You have the option to have the Crisis Alert capability notify a digital pager. When someone dials an emergency number, the system sends the extension and the location of the caller to the administered pager.

This feature sends a message containing the extension number to the administered pager. You can also administer a main number so that the pager displays the location from where the emergency call originated.

To receive a crisis alert message, you must administer at least one attendant console or one digital telephone with a **crss-alert** button.

The crisis alert call to a digital pager uses two to four trunks. The system uses:

- One trunk for the actual call
- One to three trunks to notify one to three pagers, depending on how many pagers you administer.

You must complete the following actions before a user can receive notification to a digital pager in an emergency:

- In the ARS Digit Analysis Table screen, you must have emergency numbers in the **Call Type** column set to alrt. For more information, see Setting up the emergency number.

- You must administer a **crss-alert** button on at least one of the following telephones:
  - Attendant console. For more information, see Setting up the attendant console to receive emergency notification.
  - Digital telephone. For more information, see Setting up digital telephones to receive emergency notification.

To set up Crisis Alert to notify a digital pager:

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

   The system displays the Crisis Alert System Parameters screen.
2. In the **Alert Pager** field, type `y`.

   The system displays additional Crisis Alert administration fields.
3. In the **Originating Extension** field, type a valid unused extension to send the Crisis Alert message.
4. In the **Crisis Alert Code** field, type the number that a user dials to call for emergency assistance, for example, 911.
5. In the **Retries** field, type the number of additional times that you want the system to try to send the alert message in case of an unsuccessful first attempt.
6. In the **Retry Interval (sec)** field, type the number of seconds between retries.
7. In the **Main Number** field, type the number that you want the system to display at the end of the pager message.
8. In the **Pager Number** field, type the telephone number for the pager.
9. In the **Pin Number** field, type the personal identification number (PIN), if required, for the pager. Insert pause digits (pp) as needed to pause for announcements from the pager service to complete before sending the PIN.
10. In the **DTMF Duration - Tone (msec)** field, type the number of milliseconds that the dual-tone multifrequency (DTMF) tone plays for each digit.
11. In the **Pause (msec)** field, type the number of milliseconds between DTMF tones for each digit.
12. Press `Enter` to save your changes.

Related links

Setting up the emergency number on page 692
Setting up the attendant console to receive emergency notification on page 693
Setting up digital telephones to receive emergency notification on page 693

Setting up emergency extension forwarding

About this task

If an emergency call gets disconnected, the public safety person immediately attempts to call the caller back. If the ELIN that the PSAP receives is not equivalent to the extension of the caller, the return call might ring at a different telephone. To solve this problem, you can automatically forward all incoming trunk calls, for an administered period of time, to the telephone that placed the emergency call.

Note:

You must administer time limits on the system first. If time limits are not administered, the system will not forward all incoming trunk calls because the system cannot determine what incoming trunk call is from the PSAP.

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. On the Feature-Related System Parameters screen, click **Next** until you see the **Emergency Extension Forwarding (min)** field.
3. In the **Emergency Extension Forwarding (min)** field, type the number of minutes for which you want the system to forward all incoming trunk calls to the emergency extension.

   The timer starts once an emergency call gets disconnected. This timer applies only if the Emergency Location Extension is an extension on the same system as the extension from which 911 was dialed. Customers with several systems in a location must assign multiple Emergency Location Extensions.
4. Press `Enter` to save your changes.

CAMA numbering administration for Enhanced 911

Use the CAMA Numbering - E911 Format screen to administer Centralized Automatic Message Accounting (CAMA) trunks. Also use this screen to provide Caller Emergency Service Identification (CESID) information to your local emergency system through the local tandem office.

This screen provides the CESID format by extension or number blocks. With this flexibility, multiple CESID formats can be sent over multiple CAMA trunk groups and mixed telephone numbering plans. This flexibility supports some limited conversion from non-DID to DID numbers that the Private Switch/Automatic Location Interface (PS/ALI) database usually requires.

The **System CESID Default** field defines the CESID for all extensions that are not defined in the **Ext Code** fields. The first page of this screen contains the default CESID, plus extension fields for CESID entries. Each remaining page contains additional extension fields for CESID entries.

Note:

The following procedure assumes that a CAMA trunk group is already set up. For information on how to set up trunk groups, see *Administering Avaya Aura® Communication Manager*.

Setting up CAMA numbering

Procedure

1. Type `change cama-numbering`. Press `Enter`.

   The system displays the CAMA Numbering - E911 Format screen.
2. In the **System CESID Default** field, type the CESID that the system sends over the CAMA trunk if you do not define the Ext Code fields.

   Type a number that consists of 1 to 16 digits. The default value is blank.

3. In the **Ext Len** field, type the number of digits in the extension.

   Type a number from 1 to 5. The default value is blank.

4. In the **Ext Code** field, type the leading digits or all of the digits in the extension for the specified CESID.

   If the value in the **Ext Len** field is greater than the number of digits in the **Ext Code** field, the system interprets the Ext Code as a block of digits. For example, if the value in the **Ext Len** field is 4 and the value in the **Ext Code** field is 11, the CESID serves extensions 1100 through 1199. The Ext Code [11] is for a DID block. Ext Code [126] might point a non-DID block to a nearby DID extension 5241666.

   Enter a number that consists of 1 to 5 digits. The default value is blank.

5. In the **CESID** field, type the number that identifies the calling terminal within an emergency service system.

   This field can represent a prefix to an extension, or the entire CESID.

   Enter a number that consists of 1 to 16 digits. The default value is blank.

6. In the **Total Length** field, type the total number of digits to send.

   Enter a number that consists of 1 to 16 digits. The default value is blank.

7. Press `Enter` to save your changes.

Reports for Enhanced 911

The following reports provide information about the Enhanced 911 feature:

- The Emergency Access Calls report shows the following information for each emergency call:
  - Extension
  - Event
  - Type of call
  - Time

For detailed information on this report and the associated commands, see *Avaya Aura® Communication Manager Reports*.

Considerations for Enhanced 911

This section provides information about how the Enhanced 911 feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Enhanced 911 under all conditions.

The following considerations apply to Enhanced 911:

- The Enhanced E911 feature only applies to emergency calls that go over CAMA, ISDN and SIP trunks.
- You must provide several call appearances on the last telephone in both the coverage path and the telephone hunting path of the Emergency Location Extension.
- Do not include voice mail, automated attendant, or announcement extensions for Emergency Location Extensions.

The following two consideration scenarios apply to a Survivable Remote Server (Local Survivable Processor), and to backup duplex servers. These considerations apply if the spare processor is an asynchronous transfer mode wide area network (ATM WAN), or is on a survivable remote expansion port network (EPN).

- Sending the correct ELIN to the PSAP

  Once each day, the Survivable Remote Server copies administration translations from its primary server. The system never copies translations from the Survivable Remote Server to the primary server. IP telephones can stay under the control of a Survivable Remote Server for 6 days, 10 days, or indefinitely. The length of time depends on what version of software you are running.

  If someone notifies you that an IP extension moved, update the ALI database with the physical location of the IP extension. Also change the **Emergency Location Extension** field on the IP Address Mapping screen to match the new subnetwork of the IP extension. You can also purchase an adjunct that performs this correlation and update for you.

  If the telephone registers with the Survivable Remote Server before the system copies the translations from the main server, the **Emergency Location Extension** field is still set to the old value. If the user dials 911, emergency response personnel might go to a different location for the caller instead of to the exact location.

  Never update translations directly on the Survivable Remote Server.

The following considerations apply to the Crisis Alert capability:

- The Automatic Number Identification (ANI) that the system sends to the CO might not be the same extension as the telephone that the person used to dial the emergency. If the call is disconnected and the public service person call back, the public service person calls the ANI. The public service person might not reach the caller.

  If a telephone has a **crss-alert** button assigned, the return call is answered by someone who was notified of the extension that made the emergency call. That person can then forward the return call from the public service person to the extension from which the emergency call was placed.
- Only one **crss-alert** button can appear on an attendant console or a digital telephone.
- Attendant consoles or digital telephones without a **crss-alert** button do not receive emergency notification.

Interactions for Enhanced 911

This section provides information about how the Enhanced E911 feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of E911 in any feature configuration.

- Bridged Call Appearances

  Emergency 911 calls from a bridged extension report the extension of the physical telephone, not the bridged call appearance.

- Class of Restriction (COR), Tenant Partitioning, and Facilities Restriction Level (FRL)

  COR, Tenant Partitioning, and FRL restrictions apply to CAMA trunks and 911 calls.

- Expert Agent Selection (EAS)

  When an EAS agent dials 911, the number is the number of the physical telephone, and not of the logical agent.

- Network Address Translation (NAT) devices

  If a telephone operates behind a NAT device, the ELIN is based upon the translated IP address of the telephone, and not the native IP address. If you use a NAT device, the NAT device must preserve IP subnetworks. To require a change in IP address, the E911 for wired IP telephones capability expects a move from one geographic area to another.

  For example, you have two subnetworks, 1.1.1.* and 2.2.2.*, that are mapped to two different ELINs in the IP Network Mapping screen. Both of these subnetworks operate behind a NAT device. If the NAT device maps both subnetworks of 1.1.1.* and 2.2.2.* into addresses in the range 3.3.3.*, Communication Manager cannot detect if someone moves a telephone from 1.1.1.* to 2.2.2.*.

- Non-ARS calls

  The E911 feature uses Automatic Route Selection (ARS) digit analysis to classify an outgoing call as an emergency or crisis alert call. If a user does not use ARS to dial an emergency call, the E911 feature only applies if the trunk types are CO or FX. Examples of calls that do not use ARS are:

  - Calls that use a trunk access code
  - Personal CO line button calls
  - Facility test calls
  - AAR access code calls if AAR digit analysis does not overflow to ARS

The following interactions apply to the Crisis Alert capability:

- Centralized Attendant Service (CAS)

  If CAS is enabled, the emergency alert still goes to the local attendant.

- Multiple Locations

  A crisis alert call to a digital pager is treated by the system as if the call is from Location 1. This treatment means that the pager number digits are analyzed using the Location 1 dial

plan and the Location 1 ARS Analysis Table. The system does not use the location of the station that dialed the emergency call.

- Outgoing Trunk Queuing

  If a user attempts to make an emergency call when all trunks are busy, the call does not generate an alert. If the Outgoing Trunk Queuing feature is enabled for a trunk group, the call is placed in a queue but does not generate an alert.

- Tenant Partitioning

  If Tenant Partitioning is active, stations and attendants with crisis alert buttons receive emergency notification from those callers who are within the tenant partition. If no stations or attendants with crisis alert buttons are assigned to a partition from which an emergency call originates, the system still sends a record of the call to the system printer, and to the Emergency Access Calls report.

- Terminal Self-Administration

  Users who can administer their telephones cannot disable a crss-alert button.

Requirements for integration with Emergency Location Management Solution

This section describes the requirements to enable Communication Manager to send SNMP inform messages to the Emergency Location Management Solution for non-SIP phones. For SIP phones, you must configure the Emergency Location Management Solution as an ELIN server with Session Manager. For more information, see the “Emergency call routing for H.323 visiting users” section.

Requirements are as follows:

- In the Crisis Alert System Parameters screen, in the **SNMP Inform to Notify Adjunct When DCP and H.323 Stations Go In-Service** field, type `y`.
  - Communication Manager helps the Emergency Location Management Solution to track which endpoints are in service so that if an emergency call is placed, Emergency Location Management Solution can identify the caller’s location.
  - The Emergency Location Management Solution gets equivalent registration information from Session Manager when the Emergency Location Management Solution is configured as an ELIN server.
- In the Crisis Alert System Parameters screen, in the **SNMP Inform to Notify Adjunct When SIP Station Dials Emergency Call** field, type `y`.

  Communication Manager sends inform traps to SNMP receiver when a SIP station places an emergency call.

Note:

Do not enable this field if Session Manager is handling emergency call logging to Emergency Location Management Solution.

- In the FP Traps screen, set the **Notification** field to **Inform** for SNMP v3.

  You can access the FP Traps screen from the Communication Manager System Management Interface (SMI).

- Configure Communication Manager to allow users to dial 911. 911 must be configured with call type “alrt” on the ARS Analysis screen to trigger the SNMP inform from analog, DCP, and H.323 endpoints.
  - For SIP endpoints, the Emergency Location Management Solution depends on the messages it gets from Session Manager. You must disable the second parameter at the bottom of Crisis Alert System Parameters screen.
  - Note that while *911* is the most common emergency number, the steps above work for any number configured on the ARS Analysis screen with the call type “alrt”.

Chapter 84: Enhanced Call Forwarding

Use Enhanced Call Forwarding (ECF) feature to forward incoming calls to different destinations depending on whether they are from internal or external sources.

Detailed description of Enhanced Call Forwarding

The Enhanced Call Forwarding feature requires Communication Manager Release 4.0 or later.

There are three types of Enhanced Call Forwarding:

- Use Enhanced Call Forwarding Unconditional to forward all calls
- Use Enhanced Call Forwarding Busy to forward calls when the user's line is busy
- Use Enhanced Call Forwarding No Reply to forward calls when the user does not answer the call

The user can activate or deactivate any of these three types from their phone, and can specify different destinations for calls that are from internal and external sources. Users receive visual display and audio feedback on whether or not Enhanced Call Forwarding is active.

Display messages on the phone guide the user through the process of activating and de-activating Enhanced Call Forwarding, and for viewing the status of their forwarding.

Users can choose whether they want, at any one time, Call Forwarding or Enhanced Call Forwarding activated. The regular Call Forwarding feature (called "Classic Call Forwarding" to distinguish it from Enhanced Call Forwarding) continues to be available to users and has not changed.

Each of the three types of Enhanced Call Forwarding can have different destinations based on whether a call is internal or external. Therefore, six different destinations are possible to set up:

- Enhanced Call Forwarding Unconditional - internal
- Enhanced Call Forwarding Unconditional - external
- Enhanced Call Forwarding Busy - internal
- Enhanced Call Forwarding Busy - external
- Enhanced Call Forwarding No Reply - internal
- Enhanced Call Forwarding No Reply - external.

Each of these types of call forwarding can be activated either by Feature Access Codes or by feature button.

When Enhanced Call Forwarding is deactivated, the destination number is kept. When the user activates Enhanced Call Forwarding again, the same destination number can be used without having to type it again.

When Enhanced Call Forwarding is inactive for a call, the call goes to a coverage path, if one has been set up.

Chained Call Forwarding

In Communication Manager Release 5.2, you can use the Chained Call Forwarding feature to forward the calls up to 10 hops (each calling station is considered to be one hop) using a pre-set coverage path within the same switch.

- The number of hops is in the range 3 through 10.
- A coverage path is assigned for calls forwarded to the principal or last station. This is possible when specifying a coverage path. Administer the **Station Coverage Path For Coverage After Forwarding** field to principal or last-fwd.
- Mixed use of standard call forwarding (including Call Forwarding All Calls and Call Forward Busy/Don’t Answer) and enhanced call forwarding (including Enhanced Call Forwarding Unconditional, Enhanced Call Forwarding Busy, and Use Enhanced Call Forwarding No Reply) is allowed on stations in the forwarding chain.
- Forwarding stops before the chain gets into an infinite loop or before the call gets back to the originating station.
- Call forwarding override is activated on any station in the chain. Using this feature the call can be transferred to the previous station in the chain.

Enhanced Call Forwarding feature button

The feature button cfwd-enh has been added.

- The feature button is valid only for station terminal types where feature buttons can be administered, except for attendant consoles, and have displays.
- Only one **Enhanced Call Forwarding** button with a blank destination is allowed per station. Buttons with entered extension number can be multiple-administered, but only one for the same extension number.
- The button label ECfwd will be used for stations requiring downloadable button labels. The station screen displays this button label for the button administered with the Enhanced Call Forwarding feature. The button label can be in English (default), Italian, French, or Spanish.

Enhanced Call Forwarding administration

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

Enhanced Call Forwarding can be activated and deactivated from SAT. The SAT screen displays the settings of all forwarding destinations for a station, and whether forwarding is activated or not. You can also change each forwarding destination and activate or deactivate it.

Note:

There is a new class of service entry for Enhanced Call Forwarding. On the Class of Service screen, ensure that the **Call Forwarding Enhanced** field is set to y for users to activate and deactivate the ECF feature.

The Enhanced Call Forwarding feature are also administered on the 96xxSIP and 16xxSIP telephones.

Viewing Station Status for Enhanced Call Forwarding

Procedure

1. Type `display status station xxxxx`.

   The system displays the General Status screen.

2. Page down till you find the **Enhanced Call Forwarding Destinations** field.

   You can view the forwarding destination of each active kind of ECF administered for the station.

3. Click **Enter** to exit the screen.

Enabling Feature Access Codes for Enhanced Call Forwarding

Procedure

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

   The system displays the Feature Access Codes screen.

2. In the **Call Forwarding Enhanced Activation/Deactivation** field, enter a Feature Access Code number to allow users to activate and one to deactivate Enhanced Call Forwarding.

   The FACs for activation and deactivation must be administered together. One cannot exist without the other. In contrast, the FAC for status display can exist by itself and without the others.

3. In the **Call Forwarding Enhanced Status** field, enter a Feature Access Code number to allow users to display the status of Enhanced Call Forwarding.

4. Press `Enter` to save your changes.

Enabling Chained Call Forwarding

Procedure

1. Type `change system-parameters features`. Press `Enter`.
2. On the Feature-Related System Parameters screen, click **Next** till you see the **Chained Call Forwarding?** field.
3. Set **Chained Call Forwarding?** to `y`.
4. Press `Enter` to save your changes.

Note:

Consider the Class of Restriction settings on the stations in the chain before enabling chained forwarding. The SIP stations in the chain cannot activate enhanced call forwarding.

Specifying a Chained Call Forwarding coverage path

Procedure

1. Type `change system-parameters coverage-forwarding`. Press `Enter`.
2. On the System Parameters screen, click **Next** till you see the **Chained Call Forwarding** field.
3. Specify the Maximum Number Of Call Forwarding Hops (a value between 3 and 10).
4. Set the Station Coverage Path For Coverage After Forwarding to the required path.

Note:

The field is visible only when Chained Call Forwarding is enabled.

5. Press `Enter` to save your changes.

End-user procedures for Enhanced Call Forwarding

End-users can activate or deactivate certain system features and capabilities. End-users can also modify or customize some aspects of the administration of certain features and capabilities.

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.

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.

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.

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.

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.

Interactions for Enhanced Call Forwarding

This section provides information about how the Enhanced Call Forwarding feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Enhanced Call Forwarding under all conditions. The following considerations apply to Enhanced Call Forwarding:

Agents

Agents who are logged in at a station cannot activate, reactivate or deactivate Enhanced Call Forwarding by dialing the Feature Access Code.

Attendant console

An attendant console with console permission can activate, reactivate, or deactivate Enhanced Call Forwarding in the same way stations with console permission can do, except that they cannot activate call forwarding for themselves. An attendant console can override any kind of active Enhanced Call Forwarding.

Automatic Callback

A user cannot use Automatic Callback if Enhanced Call Forwarding is active at the called station. If a user activates automatic callback before Enhanced Call Forwarding is activated at the called station, the system redirects the callback call attempt to the forwarding destination.

Bridging

The system terminates calls to a bridged appearance when Enhanced Call Forwarding No Reply is active at the user station.

Call Coverage

The priorities between Call Coverage and Enhanced Call Forwarding are the same as those between Call Coverage and Classic Call Forwarding.

Call Detail Recording

If the forced entry of account codes is required, the system does not forward calls to an off-network destination.

Call Forwarding

The following describes the interactions between Enhanced Call Forwarding and the classic Call Forwarding feature:

- Call Forwarding All Calls and Enhanced Call Forwarding Unconditional cannot be active on one station at the same time.
- Call Forwarding Busy/Don’t Answer and Enhanced Call Forwarding Busy cannot be active on one station at the same time.
- Call Forwarding Busy/Don’t Answer and Enhanced Call Forwarding No Reply cannot be active on one station at the same time.

Call Park

When a user activates Enhanced Call Forwarding and then Call Park, the Call Park is in effect at the forwarded station, not at the called station.

Chained Call Forwarding

The following summarizes interactions with chained forwarding:

When a forwarded call terminates at a station in which Enhanced Call Forwarding Unconditional is active (with both internal and external forwarding active) and chained forwarding is enabled but falls below the limit for blocking forwarding, the call is forwarded to the destination, regardless of the status of the Enhanced Call Forwarding

- Busy and No Reply features. If only one type of forwarding (internal or external) is active, then only that type of call is forwarded.
- When a forwarded call terminates at a station in which Enhanced Call Forwarding Busy is active (with both internal and external forwarding active) and chained forwarding is enabled but falls below the limit for blocking forwarding, the call is forwarded to the destination. If only one type of forwarding (internal or external) is active, then only that type of call is forwarded.
- When a forwarded call terminates at a station in which Enhanced Call Forwarding No Reply is active (with both internal and external forwarding active) and chained forwarding is enabled but falls below the limit for blocking forwarding, the call is forwarded to the corresponding destination. If only one type of forwarding (internal or external) is active, then only that type of call is forwarded.

Enhanced 911

Enhanced Call Forwarding has no effect on Enhanced 911 auto callback.

Enterprise Mobility User

The following summarizes interactions with EMU:

- EMU visited stations cannot use Enhanced Call Forwarding.
- EMU visited stations cannot activate, reactivate or deactivate Enhanced Call Forwarding.
- A user on a station with console permission can activate, reactivate, or deactivate Enhanced Call Forwarding by dialing a Feature Access Code or pushing an Enhanced Call Forwarding feature button, when the user on which the action should have the effect is in visiting mode.

Leave Word Calling

Leave Word Calling cannot be activated towards a station that has Enhanced Call Forwarding active. If Leave Word Calling was activated before the user of the called station activated Enhanced Call Forwarding, the callback attempt is redirected to the forwarded destination.

Limit number on concurrent call

Call Forwarding Busy active (both types) and Limit Number on Concurrent Call also active, the call is forwarded to the destination that is stored in the memory. If only one kind of Enhanced Call Forwarding Busy is active, then only the call corresponding to the origin call type will be forwarded.

OPTIM

Users cannot activate, reactivate, or deactivate Enhanced Called Forwarding from OPTIM stations.

Personal Central Office Line

The system does not forward Personal Central Office Line calls.

Posted Messages

The following summarizes interactions with the Posted Messages feature:

- When the Posted Messages feature is activated and Enhanced Call Forwarding is active, the display is overwritten by the posted message.
- When the Posted Messages feature is deactivated and Enhanced Call Forwarding is active, the display is overwritten by the Enhanced Call Forwarding message.
- When the Posted Messages feature is activated, activation of Enhanced Call Forwarding (whether by Feature Access Code, feature button, or the SAT) will have no effect on the display.

Priority Call

When a priority call terminates at an active Enhanced Call Forwarding station, the call is forwarded.

QSIG

Users cannot remotely activate or deactivate Enhanced Call Forwarding from a QSIG network.

Send All Calls

If a user has both Send all Calls and Enhanced Call Forwarding Unconditional active, calls to that station that can immediately be redirected to coverage are redirected. Other calls, such as priority calls, are forwarded to the designated station.

Interactions for Chained Call Forwarding

- Chained Call Forwarding is only valid, if the calls stay on the local switch. Once the call leaves the local switch the Call Forwarding Chain is broken.
- When a call is forwarded to a busy or no-reply station in which Enhanced Call Forwarding Busy is active and Chained Call Forwarding is enabled for call override, the call is forwarded to the called station for all internal and external calls.
- When a call is forwarded to a busy or out-of-service station in which Enhanced Call Forwarding Busy is active and Chained Call Forwarding is enabled and reaches the maximum number of call forwarding hops with no call coverage path set, the caller hears a busy tone.
- When calls are forwarded using chained call forwarding the calls to the forwarding station from the origination station follow a call coverage path.

Call forward override

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

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

Chapter 85: Enhanced security features

The features described in this chapter comply with the Unified Capabilities Requirements (UCR) 2013 Change 1 requirements. These features are designed for government customers.

Assured Services Admission Control

With Assured Services Admission Control (ASAC), the security administrator can:

- Assign call budgets for SIP trunk groups.
- Assign inbound and outbound call budgets for audio and video to each SIP trunk group.
- Monitor bandwidth usage using the Call Admission Control feature.
- Configure a precedence level on a SIP deskphone. Users can select a precedence level for each call on the SIP deskphone. The maximum precedence level that any given user can use is defined by his class of restriction.

Use Multiple Level Precedence and Preemption (MLPP) must be enabled to access this feature. Use MLPP to preempt the calls as necessary. For more information about enabling MLPP, see “Chapter 123: Multiple Level Precedence and Preemption”. Users with MLPP service enabled can specify the precedence level of each call they place. During call processing, this precedence level is used to assure preferential call completion of higher precedence calls within the same MLPP network domain, even if that means preempting lower precedence calls.

Trunk preemption

The security administrator can assign budget to precedence calls for call processing purpose. Communication Manager provides call budgets for SIP trunk groups. Communication Manager enforces calls in accordance with the precedence of the call and checks for the direction of the call to compare the call with the call budget. Communication Manager supports incoming call budget and outgoing call budget thresholds for SIP trunk groups. Communication Manager allows the administrator to assign thresholds. A low threshold is used to clear previous threshold alarms. Whereas, a high threshold is used to notify that the incoming or outgoing call count is at a level and that the call blocking and preemption will soon start to occur.

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 Enabling CAC sharing between Communication Manager and Session Manager. 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*.

Endpoint preemption

Users can place and receive a precedence call. Called party with no idle appearance will have lower precedence over the calls preempted by higher precedence call. For more information, refer to the endpoint documentation.

Screens for administering Assured Services Admission Control

Screen name	Purpose	Fields
Multiple Level Precedence & Preemption Parameters	To enable ASAC.	**ASAC Enabled**
Trunk Group	To assign budgets for incoming and outgoing calls.	• **Incoming Budget** • **Outgoing Budget** • **Incoming call budget high threshold** • **Incoming call budget low threshold** • **Outgoing call budget high threshold** • **Outgoing call budget low threshold**

For information about the field descriptions, see *Avaya Aura® Communication Manager Screen Reference*.

Attendant Queue Announcement

Communication Manager plays Attendant Queue Announcement (ATQA) for incoming precedence calls that are above the Routine precedence level and are placed in the attendant waiting queue.

Screen for administering Attendant Queue Announcement

Screen name	Purpose	Field
Multiple Level Precedence & Preemption	To enable Attendant Queue Announcement.	**Attendant Queue Announcement**

For information about the field description, see *Avaya Aura® Communication Manager Screen Reference*.

Communication Manager TLS support over H.248 Control Link to the Gateway

For information about the Branch Gateway CLI commands, FIPS Mode, and summary of configuration, see *Avaya Branch Gateway G450 CLI Reference*.

Screens for administering Communication Manager TLS support over H.248 Control Link to the Gateway

Screen name	Purpose	Fields
Media Gateway	To select the encryption link type for FIPS and to activate Mutual Authentication.	• **Link Encryption Type** • **Mutual Authentication**
IP Codec Set	To enable to enable the support of the RFC 4040 media service.	• **SIP 64K Data** • **Redundancy** • **Packet size (ms)**

For information about the field descriptions, see *Avaya Aura® Communication Manager Screen Reference*.

Destination Code Control

Destination Code Control (DCC) allows you to restrict outbound calls to a specific called number or a range of numbers. In the Precedence Routing Digit Analysis Table screen, the **Destination Code Control** and **Percentage IPBO Blocked** fields are used for destination code control.

For example, when you set the **Destination Code Control** to `y` and **Percentage IPBO Blocked** to `50%`, Communication Manager blocks 50% of the outbound call from the total outbound IP call budget (IPBo) when a certain number or a range of numbers is called.

If the total outbound IP call count (IPCo) reaches 50% that is equal to IPBo, and a user makes a routine call, then the routine call is denied. However, if the user makes a priority or an immediate call, then the lower precedence call in the trunk is preempted to connect the new call. DCC follows precedence rule for group or route settings on the **Preempt Method** field.

Note:

To enable the DCC feature, you must first activate DCC by using the FAC.

Note:

DCC is not applicable to flash override and flash calls. If a user makes a flash override or a flash call, the call is connected with a proper talk path.

Screens for administering Destination Code Control

Screen name	Purpose	Fields
Precedence Routing Digit Analysis Table	To activate DCC and set percentage to block outgoing calls.	• **Destination Code Control** • **Percentage IPBO Blocked**
Feature Access Code (FAC) MLPP Features	To enter the valid FAC so that DCC can be activated and deactivated.	Destination Code Control • **Activation Code:** • **Deactivation Code:**
Class Of Service	To activate DCC.	**DCC Activation/Deactivation**

For information about the field descriptions, see *Avaya Aura® Communication Manager Screen Reference*.

Failover Event Package

Communication Manager sends SUBSCRIBE messages to the primary Multi-Function Soft Switch (MFSS) and the backup MFSS and accepts subscription requests from the primary MFSS. The backup MFSS and primary MFSS use SIP OPTION messages to support failover and failback processing. When the primary MFSS fails, the control moves to the backup MFSS. However, when the primary MFSS becomes active, the control comes back to the primary MFSS.

Screen for administering Failover Event Package

Screen name	Purpose	Fields
Signaling Group	To enable failover and failback event package subscription and to set option request parameters.	• **Enable Failover Event Package Subscription** • **Failover/failback Signaling-group Pair** OPTIONS Request Parameters • **Interval between OPTIONS messages (seconds)** • **Number of OPTIONS message failure before failover** • **Number of OPTIONS message successes before failback** • **Wait time before failback (seconds)**

For information about the field descriptions, see *Avaya Aura® Communication Manager Screen Reference*.

Federal Information Processing Standard Publication

Communication Manager with Federal Information Processing Standard (FIPS) mode enabled means that CM complies with the FIPS standard encryption method.

G430 Branch Gateway and G450 Branch Gateway are certified for Level 1 compliance.

Enabling the FIPS mode

Before you begin

1. Install the latest Communication Manager software.
   - For VMware, deploy the JITC specific OVA file and then apply the latest FIPS specific service pack.
   - For System Manager, upgrade to the FIPS-only template and then install the FIPS specific service pack.
2. Obtain a third party host certificate set:
   - Communication Manager Identity certificate.
   - Trusted certificate chain. For example, the Root CA and an Intermediate CA.

     This certificate set is exchanged with the gateway or the H.323 phones during the TLS handshake. The Communication Manager server will take the role of the server in the TLS handshake with gateways and phones.

About this task

The security administrator needs to perform the following task on the Communication Manager server to enable FIPS.

Note:

The security administrators that can execute the FIPS mode command are any users that belong to the susers groups: init, inads, and craft.

Procedure

1. To enable the FIPS mode, on the Shell prompt, type the **`fips_mode enabled`** command. The security administrator is prompted for a `y` or `n`.
2. Type `y`.

   The Communication Manager server reboots automatically and the FIPS mode is enabled.

Disabling the FIPS mode

About this task

The security administrator needs to perform the following task on the Communication Manager server to disable FIPS.

Note:

The security administrators that can execute the FIPS mode command are any users that belong to the susers groups: init, inads, and craft.

Procedure

1. To disable the FIPS mode, on the Shell prompt, type the **`fips_mode disabled`** command.

   The security administrator is prompted for a `y` or `n`.

2. Type `y`.

   The Communication Manager server reboots automatically and the FIPS mode is disabled.

H.323 TLS support

Communication Manager uses TLS to encrypt the signaling channel between Communication Manager and 96x1-H.323 deskphones. After the exchange of Gatekeeper Request (GRQ) and Gatekeeper Confirm (GCF) messages is complete, the 96x1-H.323 deskphone opens a TCP/TLS channel towards Communication Manager and communication between the endpoint and Communication Manager happens through the encrypted TLS channel.

In releases before Communication Manager Release 7.0.1, you must enable FIPS mode to use TLS. With Communication Manager Release 7.0.1 or later, you can use TLS with or without enabling the FIPS mode.

Screens for administering H.323 TLS support

Screen name	Purpose	Fields
System Capacity	To check Communication Manager capacity for H.323 station support for desk phones.	**H.323 Stations via TLS**
IP Network Region	To enable the H323TLS option.	**H.323 Security Profiles**
Stations	to validate the phone certificates for TLS connection	**Require Mutual Authentication if TLS**
Status station	To check if the authentication type of the station is set to TLS.	**Authentication Type**

For information about the field descriptions, see *Avaya Aura® Communication Manager Screen Reference*.

Interactions for H.323 TLS

This section provides information about how the H.323 TLS feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of H.323 TLS in any feature configuration.

Unnamed Registration

Communication Manager sets up TLS signaling channel connections with TTS support for H.323 named registration. Unnamed registration uses the existing non-TLS signaling.

PSA feature access codes

If you use PSA feature access codes or any other method to change an existing registration from named to unnamed or vice versa, Communication Manager retains the existing TLS or non-TLS signaling channel format.

Chapter 86: Enhanced SIP Signaling

With the Enhanced SIP Signaling feature, you can:

- see a roster of conference participants
- drop the selected participants from Communication Manager based conferences
- enable audio only conferences, facilitated by Avaya Aura Meeting Exchange 6.2 and audio/video conferences, facilitated by Avaya Aura ® Conference Release 8.0 or Meeting Server 9.1
- enhance the behavior of sequenced applications in a Communication Manager Feature Server environment

The feature contains the following components:

- SIP Endpoint Managed Transfer
- RFC 4579 Conference Factory
- RFC 4579 Avaya Aura® Conferencing Release 8.0

Detailed description of Enhanced SIP Signaling

Communication Manager tandems a Refer-with-replaces SIP message from the transferring party to the transferred party. Communication Manager of the transferred party launches a new call to the transfer target. Communication Manager of the transferred party drops out of the call.

Using the Enhanced SIP Signaling feature, you can:

- see a roster of conference participants
- drop the selected participants from Communication Manager based conferences
- enable audio only conferences, facilitated by Avaya Aura Meeting Exchange 6.2 and audio/video conferences, facilitated by Avaya Aura ® Conference Release 8.0 or Meeting Server 9.1
- enhance the behavior of sequenced applications in a Communication Manager Feature Server environment

During local transfer or conference operations, Communication Manager sends the XML body to the UPDATE SIP message to other SIP parties including the parties of the current call.

This feature consists of four components:

- Tandem in-dialog Refer-replaces and Invite-replaces
- RFC 4579 Conference Factory
- RFC 4579 Conference State Event Reports
- Support for adjunct 4579 Conference Factories

SIP Endpoint Managed Transfer administration

For information on how to administer the **SIP Endpoint Managed Transfer** feature, see *Administering Avaya Aura® Communication Manager*.

Screen for Administering SIP Endpoint Managed Transfer

Screen name	Purpose	Fields
Feature-related system parameters	Enable the SIP Endpoint Managed Transfer	SIP Endpoint Managed Transfer
Enable the SIP Endpoint Managed Transfer	Enable the SIP Endpoint Managed Transfer	Network Call Redirection

Interactions for Enhanced SIP Signaling

Service Observing

With Communication Manager 6.2 and later, a call involving a 4579 conference hosted on that Communication Manager server cannot be service observed.

Chapter 87: Enterprise Mobility User

Use the Enterprise Mobility User (EMU) feature to associate the features of a user's primary telephone to a telephone of the same type anywhere within your enterprise.

Note:

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.

Detailed description of Enterprise Mobility User

EMU Enhancements for Communication Manager 4.0 or later

Starting with Communication Manager Release 4.0, the EMU feature has the following enhancements:

- Extension to Cellular Availability with EMU
- A home station of a visitor can be visited
- The EMU timer

Extension to Cellular Availability with EMU

Starting with Communication Manager Release 4.0, mobile users can use the Extension to Cellular feature to access a station that is being visited by a user of the EMU feature.

Important:

This enhancement excludes the XMOBILE EC500.

Home station of an EMU visitor can be visited

The home station of a user that is registered as an EMU visitor elsewhere in the enterprise network, can be visited by another EMU user. In the case where either user places an emergency call, both EMU registrations will be unregistered.

The EMU timer

The EMU timer can be administered on the Features-Related System Parameters screen. The EMU timer applies to the visited server only. You can administer the timer for each server in the

system. The amount of time a visitor can remain registered during a period of inactivity is entered in the **EMU Inactivity Interval for Deactivation (hours)** field. Valid entries are one to 24 hours. If the entry is left blank, the EMU timer is not used and the visited station remains registered until it becomes unregistered by other means.

System requirements for EMU

The following is a list of requirements for the EMU feature:

- QSIG must be the private networking protocol in the network of Communication Manager systems. This requirement also includes QSIG MWI.
- EMU phase 1: Communication Manager Release 3.1 and later software must be running on the home server and all visited servers.
- EMU phase 2: Communication Manager Release 4.0 and later software must be running on the home server and all visited servers. EMU phase 2 is not backward compatible with Communication Manager 3.1.
- 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 an 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 self-designating terminals.
- Uniform Dial Plan (UDP).

Note:

All systems in a QSIG network must be upgraded to Communication Manager 4.0 or later in order for the Enterprise Mobility User feature to function properly. If only some systems are upgraded, and their extensions expanded, the EMU feature might not work with the systems that have not been upgraded. See your Avaya technical representative for more information.

For optimal performance and feature functionality EMU requires,

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

EMU use and activation

To activate the EMU feature, a user enters the EMU activation feature-access-code (FAC), the extension number of their primary telephone, and a security code 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 form 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.

EMU supported telephone buttons

The following list shows the buttons that are supported by EMU:

- Abbreviated dialing (abrv-dial)
- Automatic message waiting (aut-msg-wt)
- Automatic callback (auto-cback)
- Automatic intercom (auto-icom)
- Automatic dialing (autodial)
- Bridged appearance (bridg-appr)
- Bridged Appearance of an analog telephone (abrdg-appr (Extension))
- Busy indicator (busy-ind)
- Call appearance (call-appr)
- Call forwarding (call-fwd)
- Call forwarding busy don't answer (cfwd-bsyda)
- Dial intercom (dial-icom)
- ec500
- Exclusion
- Personal central office line (per-COline)
- Send all calls (send-calls)

Up to 24 of the supported button types can be downloaded to the visited server for mapping to a visited telephone. The 24 button limitation applies to all telephones supported by EMU.

The home server sends the button state of the visited telephone. The supported states are idle, alerting with ringing or alerting without ringing, and in-use. The busy state is shown as a steady light and will not blink on the visited telephone.

EMU call processing

Calls made from a visited telephone can be processed by either the home server or the visited server. Which server processes the call depends on how the user originates the call. The home server processes any calls that are a result of a user depressing one of the buttons that were downloaded to the visited telephone. The visited server processes any calls that are placed on the visited telephone using the dial pad.

All emergency numbers must originate from the dial pad of the visited telephone to ensure that the locally applicable emergency number entered on the key pad is sent to the emergency call receipt agency. A visited telephone will be deactivated when an emergency number is dialed. The visited server determines if the call is an emergency through the Automatic Routing Selection (ARS) analysis table category of the called number. Deactivating the visited telephone gives the emergency call receipt agency the ability to make a call back to the telephone if necessary. After a visitor makes emergency call of the type emer or alrt, the EMU feature does not support use of EMU FAC for registration for an amount of time that can be administered.

EMU and the station lock feature

If the primary telephone is locked, the visited telephone cannot place outgoing calls using the Abbreviated Dial buttons or the Bridged Appearance buttons. Calls from the Abbreviated Dial buttons or the Bridged Appearance buttons are processed by the home server. The home server blocks any outgoing calls from a locked telephone.

A visited telephone can make outgoing calls if the dial pad is used. Calls from the dial pad of a visited telephone are processed from the visited server. The visited server does not know about the lock on the primary telephone.

EMU traffic considerations

The EMU feature is used by people who travel to various locations within a company’s enterprise. The number of visited telephones activated to use EMU and the subsequent traffic the EMU users generate, must be taken into consideration when designing for EMU. EMU can affect both the signaling links used for transporting the QSIG messages and the bearer network used for voice traffic. Additional trunking between the Avaya servers in the network may be required to accommodate the additional traffic. The number of additional trunks can be determined by looking at the busy hour call rate for the roaming users and the blocking rate that is supported or required.

Message waiting indication with EMU

When a visited telephone registers with a home server, the home server sends the current message waiting lamp status. The home server continues to send message waiting lamp updates to the visited server until the visited telephone is no longer registered with the home server.

Enterprise Mobility User administration

The following tasks are part of the administration process for the Enterprise Mobility User (EMU) feature:

- Configuring your system for Enterprise Mobility User
- Setting EMU options for stations
- Defining EMU calling party identification

Related links

Configuring your system for Enterprise Mobility User on page 727
Setting EMU options for stations on page 727
Defining EMU calling party identification on page 728

Preparing to administer Enterprise Mobility User

About this task

You must complete the following actions before you can administer the Enterprise Mobility User feature:

To use the EMU feature, you must have Communication Manager Enterprise Edition Release 3.1 running on Linux Media Servers.

The EMU feature does not require any other right-to-use agreements, that is, it does not have to be turned on in the license file for your system.

For other system requirements for the EMU feature, see System requirements for EMU.

Related links

System requirements for EMU on page 723

Screens for administering Enterprise Mobility User

Screen name	Purpose	Fields
Class of Service	Configuring your system for the feature	• Personal Station Access
Feature Access Code		• Enterprise Mobility User Activation • Deactivation
System-parameters features		• EMU Inactivity Interval for Deactivation (hours) • Emergency Extension Forwarding (min)
Station	Setting EMU options for stations	• Security Code • EMU Login Allowed
Trunk Group	Defining options for calling party identification	• Send EMU Visitor CPN

Configuring your system for 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.

   The PSA field applies to the primary telephone and must be set to yes for EMU.

3. Type `display feature-access-codes`.

   The system displays the Feature Access Codes screen.

4. Page down till you see the fields for Enterprise Mobility User Activation and Deactivation.

5. The feature-access-codes (FAC) 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 where you are dialing from.

   Note:

   To avoid confusion, Avaya recommends that all the servers in the network have the same EMU feature-access-codes.

6. Administer the EMU timer on the system-parameters features screen.

   The EMU timer applies to the visited server only. You can administer the timer for each server in the system. The amount of time a visitor can remain registered during a period of inactivity is entered in the **EMU Inactivity Interval for Deactivation (hours)** field. From one to 24 hours may be entered. If the entry is left blank, the EMU timer is not used and the visited station remains registered until it becomes unregistered by other means.

7. Administer the Emergency Extension Forwarding timer on the system-parameters features screen.

   The amount of time that must elapse before a visitor can log in as EMU after making emergency calls from an EMU-activated station is entered in the **Emergency Extension Forwarding (min)** field. The default value is 10 minutes.

Setting EMU options for stations

Procedure

1. Type `add station next`.

   The system displays the Station screen.

2. The following entries must be made on the Station screen:

   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 form. The security code can be up to eight numbers. No letters or special characters are allowed. Once the security code is entered, the system displays a * in the **Security Code** field.

3. On the Station screen, page down till you find the **EMU Login Allowed** field.

   The **EMU Login Allowed** field applies to the visited station and must be set to y for EMU. The valid entries to this field are y or n, with n as the default. If you set this field to y, this telephone can be used as a visited station by an EMU

4. Click `Enter` to save your changes.

Defining EMU 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. Page down till you see the **Send EMU Visitor CPN** field.

   This field controls calling party identification, that is, the extension of the primary telephone or the extension of the visited telephone that is used when a call is made from a visited telephone using the visited telephone dial pad. 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 **Send EMU Visitor CPN** display the extension of the visited telephone, you must set the field to n.

3. Select `Enter` to save your changes.

   Note:

   For QSIG trunk groups working between the visited server and the home server, the **Send Calling Number** field must be set to y for calls that originate at a visited station using a feature button.

End-user procedures for Enterprise Mobility User

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

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 88: Exclusion

With the Exclusion feature of Communication Manager, users can maintain privacy of telephonic conversations and ensure that unwanted parties cannot join the call.

You can use one of the following three modes to administer Exclusion on an endpoint:

- Manual Exclusion
- Automatic Exclusion
- Buttonless Automatic Exclusion

The Exclusion feature has been enhanced to work with the following features:

- Extension to Cellular
- Bridged Call Appearance
- Service Observing

Related links

Detailed description of Exclusion on page 730
Considerations for Exclusion on page 733
Interactions with Exclusion on page 733

Detailed description of Exclusion

Manual Exclusion

In the Manual Exclusion mode, the user presses the **Exclusion** button to activate and deactivate Exclusion. When Exclusion is activated on an endpoint, the **Exclusion** button lamp is ON.

Automatic Exclusion

In the Automatic Exclusion mode, Exclusion is activated on the endpoint when the user makes a call or answers a call. To deactivate Exclusion, the user presses the **Exclusion** button that is configured on the endpoint.

Buttonless Automatic Exclusion

In the Buttonless Automatic Exclusion mode, Exclusion is activated on an endpoint when the user makes a call or answers a call. Exclusion is deactivated when the user disconnects the call .

Related links

Exclusion on page 730

Exclusion Administration

Screens for administering Exclusion

Screen name	Purpose	Fields
Feature-Related System Parameters	• To set the value of the **Automatic Exclusion by COS** field to y. • To set the value of the **Buttonless Automatic Exclusion by COS** field to y.	• **Automatic Exclusion by COS** • **Buttonless Automatic Exclusion by COS**
Class of Service	To set the value of the **Automatic Exclusion** field of the COS group to y.	**Automatic Exclusion**
Special Applications	To set the value of the **(SA8879) - DCP Xfer Lamp Control/ Buttonless Auto Exclusion** field to y.	**(SA8879) - DCP Xfer Lamp Control/Buttonless Auto Exclusion**
Station	To add the **Exclusion** button on a station.	**Button Assignment**

Related links

Exclusion on page 730

Administering Manual Exclusion

Procedure

In the Button Assignment section of the Station screen, add the **Exclusion** button.

Related links

Exclusion on page 730

Administering Automatic Exclusion

Procedure

1. On the Feature-Related System Parameters screen, set the value of the **Automatic Exclusion by COS** field to y.
2. On the Class of Service screen, set the value of the **Automatic Exclusion** field of the COS group to y.
3. In the Button Assignments section of the Station screen, add the **Exclusion** button.

Related links

Exclusion on page 730

Administering Buttonless Automatic Exclusion

Procedure

1. On the Special Applications screen, set the value of the **(SA8879) - DCP Xfer Lamp Control/Buttonless Auto Exclusion** field to `y`.
2. On the Feature-Related System Parameters screen, set the value of the **Buttonless Automatic Exclusion by COS** field to `y`.
3. On the Class of Service screen, set the value of the **Buttonless Automatic Exclusion** field of the COS group to `y`.

Note:

Do not configure the **Exclusion** button on an endpoint on which the Buttonless Automatic Exclusion mode is administered.

Related links

Exclusion on page 730

End-user procedure for Exclusion

Using Exclusion

Procedure

1. To activate Exclusion, press the **Exclusion** button.
2. To deactivate Exclusion, either disconnect the call or press the **Exclusion** button.

Note:

Communication Manager activates Automatic Exclusion and Buttonless Automatic Exclusion when the user makes a call or answers a call. Communication Manager deactivates Buttonless Automatic Exclusion when the user disconnects the call.

Related links

Exclusion on page 730

Considerations for Exclusion

This section provides information about how the Exclusion feature functions in certain circumstances. Use this information to ensure that you receive the maximum benefits of Exclusion under all conditions. The following considerations apply to Exclusion:

- The user can activate Exclusion only on a call that is connected to the selected call appearance.
- When the user activates Exclusion on a call, none of the bridged call appearances of the parties in the call can bridge on to the call. For example, if User A calls User B, and if *either* A or B has exclusion enabled, neither A's bridges nor B's bridges can bridge on. Both User A and User B must disable exclusion to let any bridged party join the call.
- Only the user who has activated Exclusion on a call can deactivate Exclusion on the same call.
- In the Automatic Exclusion mode, Exclusion is deactivated when the user disconnects the call or presses the **Exclusion** button that is configured on the endpoint.
- If a station is administered in the Manual Exclusion mode or the Automatic Exclusion mode, the user can press the **Exclusion** button configured on the endpoint to switch between Exclusion activation and deactivation states.
- When a user activates Exclusion on a conference call, only the bridged call appearances and the EC500 extension of the user are dropped from the call. For example, if User A calls User B, and one of User B's bridges join the call, *only* B can kick off B's bridge using the exclusion button. When A presses exclusion, B's bridges remain on the call.
- When a user activates Exclusion, the appearances associated with the prime call appearance are dropped from the call. For example, Station A has bridged call appearances on Station A1 and Station A2. Station B is used to call Station A. Station A1 is used to answer the call. Station A and Station A1 bridge on to the call, and a four-party conference takes place. When Exclusion is activated at Station A2, both Station A and Station A1 are dropped from the call.

Related links

Exclusion on page 730

Interactions with Exclusion

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

Extension to Cellular

- When a user activates Exclusion at the principal endpoint, the EC500 extension of the endpoint cannot join the call using Active Call FNE.

- If a user activates Exclusion and performs the Hold operation on the call, the EC500 extension of the principal station can join the call by using Held Appearance Select FNE. After the EC500 extension joins the call, Communication Manager restores Exclusion on the call.
- If a user activates Exclusion at the principal endpoint, the principal endpoint can extend the call only when the values of the **Extend Call/EC500 Bridging with Exclusion?** field on the Feature-related System Parameters screen and the value of the **(SA8879) — DCP Xfer Lamp Control/Buttonless Auto Exclusion** field on the Special Applications screen is y.

Bridged Call Appearance

- When Automatic Exclusion is activated at the principal endpoint and the bridged call appearances bridge on to the call, Communication Manager does not activate Exclusion on the bridged call appearances. For example, Station A has bridged call appearances on Station A1 and Station A2. Station B is used to call Station A. When the call is answered at Station A, Communication Manager activates Exclusion on Station A. Station A deactivates Exclusion. When Station A1 bridges on to the call, the call goes into a three-party conference, and Communication Manager does not activate Exclusion on Station A1.

Hold

- When the **Automatic Exclusion** or **Buttonless Automatic Exclusion** field on the Feature-Related System Parameters screen is set to y, and Exclusion is activated and the user performs the Hold operation on a call, the appearances associated with the prime call appearance can join the call. After the appearances join the call, Communication Manager restores Exclusion.
- When a user activates Manual Exclusion on a call and then performs the Hold operation, the appearances associated with the prime call appearance cannot join the call.

Conference and Transfer

- When Exclusion is activated on a conference call, the host of the conference can complete the conference. After the Conference operation is completed, Communication Manager restores Exclusion.
- When Exclusion is activated on a conference call, the user can perform the Transfer operation. After the Transfer operation is completed, Communication Manager restores Exclusion.

Group Page

A Group Page paging member cannot activate Exclusion. Communication Manager does not activate Automatic Exclusion and Buttonless Automatic Exclusion for Group Page members. Communication Manager activates Automatic Exclusion and Buttonless Automatic Exclusion on the originator of the paging group call.

Service Observing

- A service observer can bridge on to a call that has Exclusion activated only when the value of the **SSC/SO allowed** field is set to y. This interaction applies to the Listen Only and the Talk/Listen modes of Service Observing.
- When Exclusion is activated on a call, the service observers who are connected to the call are dropped. This interaction is applicable to the Listen Only and the Talk/Listen modes of Service Observing.

Single Step Conference

- An invisible Single Step Conference party cannot join a call that has Exclusion activated when the value of the **SSC/SO allowed** field is set to `n` . A visible Single Step Conference party cannot join a call that has Exclusion activated on it regardless of the value of **SSC/SO allowed** field.
- When Exclusion is activated on a call, none of the Single Step Conference parties connected to the call are dropped. This interaction is applicable to the Listen Only and the Talk/Listen modes of Service Observing.

Multi-Device Access

- Only the MDA device that is used to answer a call can be used to activate Exclusion on that call.
- Only the MDA device that is used to activate Exclusion can be used to deactivate Exclusion.
- Once Exclusion is activated on a call, no other MDA device can be used to join the call.
- Automatic Exclusion or Buttonless Automatic Exclusion is activated on a call when the call is answered from any one of the MDA devices. The user can deactivate Exclusion by pressing the **Exclusion** Button or by disconnecting the call.

Related links

Exclusion on page 730

Chapter 89: Extended User Administration of Redirected Calls

Use Extended User Administration of Redirected Calls to change your lead-coverage path or your call forwarding extension from any onsite or off-site telephone.

Detailed description of Extended User Administration of Redirected Calls

Using Extended User Administration of Redirected Calls, a user can change the lead coverage path or the call forwarding extension from any on-site or off-site telephone.

The Extended User Administration of Redirected Calls feature does not change the Call Coverage, Call Forwarding All Calls, or Call Forwarding Busy/Don't Answer features. Extended User Administration of Redirected Calls merely allows a user to select between one of two previously administered coverage paths, or to change the forwarding extension from any telephone.

A user must enter both a Feature Access Code (FAC) and a Station Security Code (SCC) to use Extended User Administration of Redirected Calls from an:

- On-site telephone that is unassigned to the user
- Off-site telephone

Note:

You must dial the SSC number only if the **Console Permissions** field on the COS screen is `n`.

Security alert:

The system logs invalid extensions and invalid SCCs as security violations. If you enable Security Violation Notification (SVN), the system displays the following information on the Monitor Security-Violations Station Security Codes screen or report:

- The extension or the incoming trunk from which the user dialed the command sequence
- The FAC

- The command string that the user dialed

For more information, see the Security Violation Notification.

Related links

Security Violation Notification on page 1184

Disabling the telecommuting access extension

About this task

If you want to quickly disable Extended User Administration of Redirected Calls for all users, change the **Telecommuting Access Extension** field on the Telecommuting Access screen to blank.

Extended User Administration of Redirected Calls and DCS

If your users operate in a Distributed Communication System (DCS) environment, you must assign a different telecommuting access extension to each server. You must tell your users which extension to use for telecommuting access.

A user can use Extended User Administration of Redirected Calls from any of the DCS nodes. A user must dial the telecommuting access extension of the node on which the user telephone is defined, before the user can use any of the extended FACs.

Extended User Administration of Redirected Calls and Class of Service

The table on page 737 shows the relationship between Class of Service (COS) and the ability to forward calls from the telephone that is assigned to a user without a security code, or from any onsite or off-site telephone with a security code.

Table 76: COS and Extended User Administration of Redirected Calls and Call Forwarding

If the COS of the user is set as follows:				The user can:	
Call Fwd All COS	**Call Fwd B/DA COS**	**Extended Call Fwd Activate All COS**	**Extended Call Fwd Activate Busy D/A COS**	**Forward calls from the user telephone without a security code**	**Forward calls from the user telephone or from another telephone with a security code**
Yes	Yes	Yes	Yes	Yes	Yes
No	No	Yes	Yes	No	Yes
Yes	Yes	No	No	Yes	No

Extended User Administration of Redirected Calls and COR

The user Class of Restriction (COR) controls the use of the change coverage option of Extended User Administration of Redirected Calls. If the **Can Change Coverage** field on the Class of

Restriction screen is set to y, the user can use the FAC for Change Coverage Feature Access Code to change the coverage option.

Extended User Administration of Redirected Calls from an off-site telephone

To use Extended User Administration of Redirected Calls from an off-site telephone, a user must first access the telecommuting access extension. If the user makes a request through Direct Inward Dialing (DID), the user must precede the extension with the correct public network prefix. If the user makes the request through a trunk group that is dedicated to remote access, the user must dial the public network number for the trunk group.

The system provides dial tone after the user accesses the telecommuting access extension. After the dial tone, the user can enter only one of the four following FACs that are associated with Extended User Administration of Redirected Calls:

- Extended Call Fwd All Activate
- Extended Call Fwd Busy D/A Activate
- Extended Call Fwd Deactivation
- Change Coverage

Extended User Administration of Redirected Calls administration

The following task is part of the administration process for the Extended User Administration of Redirected Calls feature requires the following hardware:

- Assigning an SSC for user administration of redirected calls
- Assigning a telecommuting access extension
- Assigning the extended FACs
- Assigning a Class of Service (COS) for extended forwarding
- Assigning a COR to change coverage from an onsite or an off-site telephone

Related links

Assigning a telecommuting access extension on page 740
Assigning the extended FACs on page 740
Assigning a Class of Service (COS) for extended forwarding on page 741
Assigning a COR to change coverage from an onsite or an off-site telephone on page 741
Assigning an SSC for user administration of redirected calls on page 741

Preparing to administer Extended User Administration of Redirected Calls

Procedure

1. Ensure that the feature is enabled for your system.
2. Assign a telecommuting access extension for your system.
3. Assign the following extended Feature Access Codes (FACs) for your system.
   - Extended Call FWD Activates Busy D/A
   - Extended Call Fwd Activate All
   - Extended Call Fwd Deactivation
   - Change Coverage
4. Assign the Class of Service (COS) for extended forwarding.
5. Assign a Class of Restriction (COR) by which a user can change coverage from an on-site or an off-site telephone.
6. View the Optional Features screen, and ensure that the **Cvg Of Calls Redirected Off-Net** field is set to y.

   If the **Cvg Of Calls Redirected Off-net** field is set to n, your system does not support the Extended User Administration of Redirected Calls feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Extended User Administration of Redirected Calls, or to open a service request.

   To view the Optional Features screen, enter `display system-parameters customer-options`.

Screens for administering Extended User Administration of Redirected Calls

Screen name	Purpose	Fields
Feature Access Code (FAC)	Specify the FAC for extended administration of Call Forward Busy/ Don't Answer and Call Forward All Calls	• Extended Call Fwd Activate Busy D/A All • Extended Call Fwd Activate Busy D/A All Deactivation
	Specify the FAC for extended administration of the lead-coverage path	Change Coverage
Class of Restriction	Administer a COR used for extended administration of the lead-coverage path	Can Change Coverage

Table continues…

Screen name	Purpose	Fields
Class of Service	Administer a Class of Service (COS) that allows the use of extended administration of Call Forward Busy/ Don't Answer and Call Forward All Calls	• Extended Forwarding All • Extended Forwarding B/DA
Optional Features	Enable Extended User Administration of Redirected Calls	Cvg Of Calls Redirected Off-Net
Station	Specify a Station Security Code (SSC) for a user	• Security Code • Coverage Path 1 • CoveragePath 2
Telecommuting Access	Define a telecommuting access extension for the system	Telecommuting Access Extension

Assigning a telecommuting access extension

Procedure

1. Enter `change telecommuting-access`.
2. In the **Telecommuting Access Extension** field, type an extension that conforms to your system dial plan. This extension can consist of 1 to 7 digits.
3. Click **Enter** to save your changes.

Assigning the extended FACs

Procedure

1. Enter `change feature-access-codes`.
2. In the **Change Coverage Access Code** field, type the FAC to change a coverage path from an onsite or an off-site telephone.
3. Click **Next** until you see the **Extended Call Fwd Activate Busy D/A All** field.
4. In the **Extended Call Fwd Activate Busy D/A All** field, type the FAC to activate Call Forwarding from an onsite or an off-site telephone.
5. In the **Call Fwd Activate Busy D/A All Deactivation** field, type the FAC to deactivate Call Forwarding from an onsite or an off-site telephone.
6. Select **Enter** to save your changes.

Note:

The system displays the FACs only if the **Cvg Of Calls Redirected Off-Net** field on the Optional Features screen is set to y.

Assigning a Class of Service (COS) for extended forwarding

Procedure

1. Enter `change cos`.
2. In the **Extended Forwarding All** field, type `y` in the column of each COS for extended Call Forwarding.
3. In the **Extended Forwarding B/DA** field, type y in the column of the COSs for extended Call Forwarding Busy/Don't Answer.
4. Select **Enter** to save your changes.

Assigning a COR to change coverage from an onsite or an off-site telephone

Procedure

1. Enter `change cor n`, where *n* is the number of the COR to which you want to assign a COR to change coverage from an onsite or an off-site telephone.
2. In the **Can Change Coverage** field, perform one of the following actions:
   - If you want users to change coverage from an onsite or an off-site telephone, type `y`.
   - If you do not want users to change coverage from an onsite or an off-site telephone, type `n`.
3. Select **Enter** to save your changes.

Assigning an SSC for user administration of redirected calls

Procedure

1. Type `change station n`, where *n* is the number of the user extension to which you want to assign an SSC. Press `Enter`.

   The system displays the Station screen.
2. In the **Security Code** field, type `SSC`.

   The **Minimum Security Code Length** field on the Feature-Related System Parameters screen determines the length of the SSC.

   The user must have a Coverage Path 1 and a Coverage Path 2. For more information, see the Call Coverage feature.
3. Press `Enter` to save your changes.

End-user procedures for Extended User Administration of Redirected Calls

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Changing the call coverage path by using Extended User Administration of Redirected Calls

Before you begin

Check the value of the **Console Permissions** field on the COS screen.

Procedure

1. Dial the Feature Access Code (FAC) for Change Coverage.

   You hear a dial tone.

2. Dial the extension of the station that requires change in the coverage path.

   If the value of the **Console Permissions** field on the COS screen is `y`, do not perform Step 3 procedure and proceed to Step 4.

3. If the **Console Permissions** field on the COS is `n`:

   a. Press the pound key (#).

   b. Dial the Station Security Code (SSC) number of the extension.

   c. Press the pound key (#).

   Tip:

   If you do not want to wait for the inter-digit timer to collect further digits, press the pound key (#).

4. To change the coverage option, dial one of the following numbers:

   - `1` for the first coverage option.
   - `2` for the second coverage option.

   You hear a confirmation tone. This tone indicates that the coverage is changed.

Activating Call Forward by using Extended User Administration of Redirected Calls

Before you begin

Check the value of the **Console Permissions** field on the COS screen.

Procedure

1. Dial the Feature Access Code (FAC) for Change Coverage.

   You hear a dial tone.

2. Dial the extension of the station that requires the activation of the Call Forward feature.

   If the value of the **Console Permissions** field on the COS screen is `y`, do not perform Step 3 procedure and proceed to Step 4.

3. If the value of the **Console Permissions** field on the COS screen is `n`,

   a. Press the pound key (#).

   b. Dial the Station Security Code (SSC) number of the extension.

   c. Press the pound key (#).

   You hear a dial tone.

   Tip:

   If you do not want to wait for the inter-digit timer to collect further digits, press the pound key (#).

4. Dial the forwarded-to extension.

   You hear a confirmation tone. The tone indicates that the forwarded-to extension is valid.

Deactivating Call Forward by using Extended User Administration of Redirected Calls

Procedure

1. Dial the **Extended Call Fwd Activates Busy D/A All Deactivation** FAC.

   The system generates a dial tone to prompt for the extension.

2. Dial the extension of the station that requires deactivation of the Call Forward feature.

   If the value of the **Console Permissions** field on the COS screen is `y`, do not perform Step 3 procedure and proceed to Step 4.

3. If the value of the **Console Permissions** field on the COS screen is `n`,

   a. Press the pound key (#).

   b. Dial the Station Security Code (SSC) of the extension.

   c. Press the pound key (#).

   You hear a dial tone.

   Tip:

   If you do not want to wait for the inter-digit timer to collect further digits, press the pound key (#).

4. Dial the forwarded-to extension.

   You hear a confirmation tone. The tone indicates that the forwarded-to extension is valid.

Interactions for Extended User Administration of Redirected Calls

This section provides information about how the Extended User Administration of Redirected Calls feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Extended User Administration of Redirected Calls in any feature configuration.

Call Coverage

Users can use the Extended User Administration of Redirected Calls feature to change the lead coverage path.

The system denies an attempt to activate Send All Calls, if the coverage criteria of the currently active coverage path restrict Send All Calls.

If a user activates Send All Calls, and then changes the coverage path to a path that restricts Send All Calls, the **Send All Calls** button remains lit. If the user changes the coverage path back to a path of Send All Calls, Send All Calls is automatically available to the user.

Call Forwarding

When Call Forwarding is active, the status lamps for the active features for that extension are lit. When Call Forwarding is deactivated, the status lamps for both **Call Forward All Calls** and **Call Forward Busy/Don’t Answer** buttons for that extension are not lit.

The system does not support forwarding to an off-network location.

Distributed Communications System (DCS)

You must assign a different telecommuting access extension for each server. Users can use Extended User Administration of Redirected Calls from any of the DCS nodes. The user must dial the extension of the node on which the telephone of the user is defined before the user dials the FAC.

Security Violation Notification (SVN)

If you enable SVN, the system tracks and reports Extended User Administration of Redirected Calls security violations for SSCs.

Tenant Partitioning

The system denies the request if the tenant number of the extension that a user dials is inaccessible by the tenant number from which the user dials an FAC for Extended User Administration of Redirected Calls.

If a user dials an FAC from an onsite telephone, the tenant number of the telephone from which the user dials the FAC must have access to the tenant number of the extension that the user dials.

If the user dials the FAC from an off-site telephone, the tenant number of the incoming trunk must have access to the tenant number of the extension that the user dials.

Chapter 90: Extended security hardening

You can harden Communication Manager 7.1.2 and later to reduce vulnerabilities and enhance the security of the Communication Manager application. Hardening the Communication Manager provides an additional security mechanism to your application.

If you are upgrading from Communication Manager Release 7.1.2 or later to Communication Manager Release 8.0 or later, the settings for the following commands are automatically carried forwarded to Communication Manager Release 8.0 or later:

- Clamav
- AIDE
- Auditd

For Selinux settings, a prompt appears when you log in to Communication Manager Release 8.0 or later. Verify the restored values, and if the values do not match, you must run **`setCMSelinux`** command to set the selinux to the correct value. Any MUDG hardening using MUDG_part1 or its alias, setCMHardening must be done again in Communication Manager Release 8.0 or later.

Supported security hardening grades

Communication Manager supports standard and hardened installation types from a security point of view. Standard installation is the default installation, and no additional action is required to set up this configuration. The table shows the hardening commands needed to set up a hardened installation.

The two security hardening grades are compared in the following table.

Security attribute	Standard installation	Hardened installation	Hardening command
VM Configuration Hardening See point 1 in the Note at the bottom of the table.	Y	Y	N
Password Management	Y	Y (more restrictive)	setCMHardening

Table continues…

Security attribute	Standard installation	Hardened installation	Hardening command
Login and Session Management	Y	Y (more restrictive)	setCMHardening
System and Application Files Hardening	Y	Y (more restrictive)	setCMHardening
Certificate Management	Y	Y	SMI Certificates Pages
Support TLS	Y	Y	SMI Server Access Page
FIPS 140-2 Compliance	N	Y	fips_mode
Multifactor Authentication (PIV and CAC support)	N	Y	Manual Configuration Required See point 2 in the Note at the bottom of the table.
SELinux Enabled	N	Y	setCMSelinux
Linux OS Auditing	N	Y	setCMAuditd
AIDE (File Tampering Prevention)	N	Y	setCMAide
Clam AV anti-virus See point 3 in the Note at the bottom of the table.	N	Y	setCMClamav

Note:

1. VM ESXi VMX file hardening is applied as part of Solution Deployment Manager (SDM) deployment.
2. Requires root access to configure the use of authorized keys from “Smart” card for user accounts.
3. Requires compatible Security Service Pack with latest Communication Manager release. (release 7.1 is still in market. Security Service Pack earlier to the mentioned release will not work for the feature).

For detailed information on the associated commands, see the *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Chapter 91: Extension to Cellular

Use the Extension to Cellular feature to extend your office calls and Communication Manager features to a cellular telephone.

For user information for Extension to Cellular, see the *Avaya Extension to Cellular User's Guide*.

For information on administration screens, see *Administering Avaya Aura® Communication Manager*.

Detailed description of Extension to Cellular

Extension to Cellular overview

The Avaya Extension to Cellular feature provides users with the capability to have one administered telephone that supports Communication Manager features for both an office telephone and up to four outside telephones. An office telephone is a telephone that is directly under the control of Communication Manager, such as a desk telephone in an office. The outside telephone is a cellular or wireless telephone and is referred to in this text as a *cell phone.* Extension to Cellular works with any type of wireless or cellular service.

With Extension to Cellular, users can receive and place official calls anywhere, at any time, even if the users are not in the office. In addition, users can also access Communication Manager features through the cell phone. Users can enable and disable Extension to Cellular so that the cell phone does not always receive office telephone calls. Users can also switch between the cell phone and office telephone during an ongoing Extension to Cellular telephone call.

When Extension to Cellular is administered and active, a call to the office telephone extension alerts both the office telephone and the cell phone simultaneously. In addition, Extension to Cellular maintains consistency in contact information. The cell phone takes on the identity of the office telephone when calls are made from the cell phone to another number on the same switch as the cell phone sends the caller ID information of the office telephone of the caller. Therefore, calls from the cell phone appear to be from the office telephone number.

A user operates a cell phone as if it were a standard, caller ID-enabled telephone extension connected directly to an Avaya server running Communication Manager. The cell phone acts as an extension because the cell phone is mapped to the main office telephone. All other types of cell phone calls, such as direct calls to and from the published cell phone number, are not affected by Extension to Cellular. The cell phone performs exactly as it did before enabling Extension to

Cellular. If your Cellular Service Provider (CSP) provides this service, Extension to Cellular is always enabled. You can also enable or disable Extension to Cellular by using a Feature Name Extension (FNE), as described in Setting up Feature Name Extensions set.

Note:

EC500 and CSP work only with ISDN-PRI, ISDN-BRI, H.323, Multi Frequency Compelled (MFC), and SIP trunks.

Cellular service providers who resell the Extension to Cellular service use the CSP or SPFMC (Service Provider Fixed-Mobile Convergence for dual mode phones) application type. CSP/SPFMC support ISDN, H.323, and SIP trunks. CSP/SPFMC is essentially the same as the Extension to Cellular application. Unlike Extension to Cellular, CSP/SPFMC is always enabled. With CSP or SPFMC, users cannot disable Extension to Cellular.

The Extension to Cellular feature also supports Fixed Mobile Applications (FMC), Public Fixed Mobility (PBFMC), and Private Fixed Mobility (PVFMC). The FMC applications are used for wireless endpoints that support a one-X Mobile Client application that has two modes called SMode (Single Mode) and DMode (Dual Mode). The FMC applications (PBFMC, PVFMC, and SPFMC) are the only OPTIM applications that support the CTI Mobility Integration feature.

When both the PBFMC and the PVFMC applications are administered for a station, incoming calls to that station are forked to both the public and private destinations specified in the station-mapping administration list. If the private FMC application receives a message indicating that the far-end has answered the call, Communication Manager cancels the call on the public FMC application. Reception of an alerting indication means that the wireless endpoint must be present in the private wireless network and therefore cannot be in the cellular network.

See also Application RTUs for Fixed Mobile Convergence.

Related links

Setting up Feature Name Extensions set on page 776
Application RTUs for Fixed Mobile Convergence on page 750

Conditional Call Extending Feature

Conditional Call Extending used to administer up to six different independent settings, controls which type of calls to extend when EC500 is enabled. You can administer the Conditional Call Extending settings and apply these settings to a specific application instead of the station as a whole. In addition to the administrator, the user can also set the Conditional Call Extending settings. Conditional Call Extending feature is used by FMC applications such as PBFMC, PVFMC, and SPFMC. This feature is not supported for PVFMC application when administered as a dual mode pair (DMX) with a ONE-X application. Conditional Call Extending feature is also not supported for OPS application.

The six different independent settings to control the type of call to extend are as follows:

- Standard calls to the station
- Calls covered or forwarded to the station
- Calls to the station through a hunt group

- Intercom calls to the station
- Priority calls to the station
- Calls restricted by a Class of Restriction (COR) permission matrix

Shared Voice Connections Feature

With Shared Voice Connections, two voice calls can share a single trunk connection between the cell phone and the PBX. For example, if the user is talking to someone and they need to put the call on hold, using the cell phone second call appearance the user dials the Hold FNE (or uses the FMC application). The first call looks to be dropped at the cell phone, but is really on hold in Communication Manager. When you initiate or answer a second cell phone call, the first call is put on hold at the PBX and its voice connection is dropped; it is combined with the new active call as a shared connection. You can access and connect the held call using Recall FNE. You can use shared voice connection option only with the FMC applications such as PBFMC, PVFMC, and SPFMC.

Sharing Mappings among Communication Manager PBXs

Using the Sharing Mappings feature, the station name and the station mapping information can be shared across multiple Communication Manager. When you call into a PBX other than your own, the called station displays your name and number as administered on your own PBX. Extension to Cellular users can be recognized on another PBX where they are not administered. When the PBX acquires the shared information, it creates a temporary mapping to associate the shared cell phone number with the shared extension and the station name. Any calls with a calling number matching a temporary mapping use the shared station name and displays the extension for incoming call.

SPFMC OPTIM Application

Communication Manager supports PBFMC RTU. An SPFMC Application that is used for support of service providers offering Extension to cellular is tied to the PBFMC RTU. An SPFMC application can be associated with a PVFMC application to support a dual-mode cell phone. You can define the application to be part of a dual-mode pair. There may be two sets of dual-mode pairs.

Application RTUs for Fixed Mobile Convergence

The Fixed Mobile Convergence (FMC) application is used for wireless endpoints that support one-X Mobile Client.

FMC supports two modes called the following:

SMode (Single Mode): Provides functionality for phones operating in the public cellular network. The existing RTU for Extension to Cellular can continue to be used to support the one-X Mobile Client application.

DMode (Dual Mode): Provides functionality for dual mode wireless phones that operate in both the public cellular network and in a wireless SIP network.

An Extension to Cellular license provides an EC500 RTU or a Cellular Service Provider (CSP) RTU. A Single mode license provides an EC500 or CSP or SPFMC RTU or PBFMC RTU. A Dual Mode license provides an EC500 RTU CSP or SPFMC RTU or PBFMC RTU (single mode) and a private FMC (PVFMC) (dual mode) RTU.

Each dual-mode telephone requires two applications. The PBFMC application works similarly to Extension to Cellular and supports the cellular aspects of the dual-mode phone. The PVFMC application supports the SIP WiFi aspects of the dual mode phone. The two applications work together to support mobility features such as handover. If the dual mode endpoint is in both the WiFi and GSM range, WiFi gets priority and the call to the endpoint is routed through WiFi.

When you administer both public and private FMC applications for a station, calls to that station extend to public and private destinations as specified in administration for station mapping.

ARS/AAR routing with Extension to Cellular

On Communication Manager, with the Extension to Cellular feature, extensions can be remotely connected over an ISDN trunk. Unlike traditional off-premises extensions, the stations are not tied to fixed channels on the T1/E1 interface. Instead, channels are allocated dynamically with each new call, providing significantly more efficient use of the T1/E1 interfaces through traffic engineering.

Routing of Extension to Cellular extended calls takes the following path:

1. ARS (or AAR) digit conversion is applied to the administered dial prefix and cell phone number.
2. ARS (or AAR) analysis is applied to the result of Step 1.
3. The ARS (or AAR) analysis selects a routing pattern.
4. Each entry in the routing pattern is tried in order. However, if the trunk group for a particular entry is non-ISDN or non-IP and not R2FMC, the trunk group is skipped.
5. A trunk group is chosen for the Extension to Cellular call and the call is sent.

If no trunk is available, the Extension to Cellular call is not extended. However, the original call is unaffected. The caller continues to hear ringback tone either until voice mail covers the call or the caller disconnects.

When the multiple locations customer option is enabled on Communication Manager, location-based routing tables are chosen as follows:

For calls sent to the cell phone the location used is:

1. The location administered on the off-pbx station-mapping form
2. The location of station

For calls dialed from the cell phone the location used is:

1. The location administered on the off-pbx station-mapping form
2. The location administered on the station form. Communication Manager uses the location of the incoming trunk if the location field on the station form is left blank.

Basic Extension to Cellular operation

Calls to the desk set also ring on an associated cell phone. This is called termination mapping.

When an Extension to Cellular call is made to the cell phone:

- Status of office telephone shows both the Extension to Cellular status and the regular station status.
- Any other station linked to the call as part of a bridge or temporary bridge can bridge on to the cell phone call.
- The same calling number presented to the desk set is sent to the cell phone

When a user answers a call with a cell phone, Communication Manager treats the call as a local answer of a station.

Sometimes users do not require physical office numbers. Therefore, you can map the cell phones to an administration without hardware (AWOH) extension.

Extension to Cellular depends on ISDN PRI/BRI, R2MFC or SIP facilities to the PSTN. The customer must have ISDN PRI/BRI , R2MFC or SIP trunks enabled and have the appropriate media module and the service from the PSTN.

Extension to Cellular users can access standard cellular features such as incoming call waiting and caller ID. If the cell phone and cellular network support call waiting, you can administer Extension to Cellular to deliver calls to a busy cell phone. Users can use cell phone features, such as swapping calls or conference calls, to answer the second call and manipulate the two calls.

If the cell phone and network support calling number identification, Communication Manager delivers the calling number to the cell phone. For calls that originate internally, the calling number can be presented in either the national numbering plan format or as an extension. You can control the number format through the administration of calling number identification. Note, some networks cannot carry an extension as a valid number. Some cell phone networks only pass calling number information in the national format, while others are more flexible.

Call Detail Recording with Extension to Cellular

Extension to Cellular provides Call Detail Recording (CDR) options for calls to cellular/external telephones. Use the CDR feature to record information on incoming, outgoing, and tandem calls for each trunk group that you administer for CDR. The system records information on each trunk-group call and each station-to-station call. Call records might be desirable if you want to track calls to cell phones for reporting or charging purposes. Calls to cell phones are treated as either trunk calls or calls to an internal station extension. However, CDR is not generated for Feature Name Extensions (FNEs) or Feature Name URI's (FNUs).

For more general information, see the Call Detail Recording feature description in this document.

For more information about administering Call Detail Recording, see *Administering Avaya Aura® Communication Manager*.

Related links

Call Detail Recording on page 384

CDR Reports for Extension to Cellular Calls

The originating extension of the call is either:

- The office telephone extension to which the Extension to Cellular station is mapped
- The cell phone number

Extension to Cellular telephones are tagged on an intra-call CDR report when the call originates from an Extension to Cellular telephone. All Extension to Cellular CDR reports have an account code consisting of all 8s. An example account code is 8888. The code length can be up to the maximum administered length of the CDR Account Code.

If the principal station is being tracked in the Intra-Switch CDR report, a CDR record is generated for the station-side of the call. The CDR record contains the calling and called parties. This report is in addition to the CDR report for the Extension to Cellular call.

Two CDR reports can be generated for each Extension to Cellular call:

- The trunk CDR record containing the cell phone number
- The principal and the intraswitch CDR record containing the principal office telephone and the original calling party

When an intraswitch call and a trunk call originate at an Extension to Cellular telephone, only the trunk call gets reported in the CDR.

Enhanced CDR output for OPTIM originating calls

Table 77: Enhanced CDR output for OPTIM originating calls

CDR Report? field on the Trunk Group screen	CDR for Calls to EC500 Destination field on the Configuration Set screen	OPTIM (or Principal in bridging setup) in the Intra-Switch CDR screen	Outcome	
			Type of CDR records (Trunk or Intra-switch)	Contents of interest
Yes	Yes	No	Trunk CDR	Destination + cell phone/SIP phone number + principal + OPTIM tag (88888)
Yes	Yes	Yes	1 CDR record (Trunk or Intra-switch)	Trunk CDR: Destination + cell phone/SIP phone number + principal + OPTIM tag Intra CDR: Destination + desk set extension
Yes	No	No	No CDR	N/A

Table continues…

CDR Report? field on the Trunk Group screen	CDR for Calls to EC500 Destination field on the Configuration Set screen	OPTIM (or Principal in bridging setup) in the Intra-Switch CDR screen	Outcome	
			Type of CDR records (Trunk or Intra-switch)	Contents of interest
Yes	No	Yes	Intra-switch CDR	Destination + desk set extension
No	Yes	No	No CDR	N/A
No	Yes	Yes	Intra-switch CDR	Destination + desk set extension
No	No	No	No CDR	N/A
No	No	Yes	Intra-switch CDR	Destination + desk set extension

Enhanced CDR output for OPTIM terminating calls

Table 78: Enhanced CDR output for OPTIM terminating calls

CDR Report? field on the Trunk Group screen	CDR for Calls to EC500 Destination field on the Configuration Set screen	OPTIM (or Principal in bridging setup) in the Intra-Switch CDR screen	Outcome	
			Type of CDR records (Trunk or Intra-switch)	Contents of interest
Yes	Yes	No	Trunk CDR	Cell phone/SIP phone number + principal + OPTIM tag (88888)
Yes	Yes	Yes	1 CDR record (Trunk or Intra-switch)	Trunk CDR: Cell phone/SIP phone number + principal + OPTIM tag Intra CDR: Principal + calling party
Yes	No	No	No CDR	N/A
Yes	No	Yes	Intra-switch CDR	Principal + calling party
No	Yes	No	No CDR	N/A
No	Yes	Yes	Intra-switch CDR	Principal + calling party
No	No	No	No CDR	N/A
No	No	Yes	Intra-switch CDR	Principal + calling party

Call filtering with Extension to Cellular

With call filtering, you can manage cell phone costs by limiting the call type extended to the cell phone. Call filtering is based on the incoming call type received at the cell phone. You can choose to deliver external calls, internal calls, all calls, or no calls. All these calls can be delivered on a per-user basis.

Using Internal call filtering, the switch can extend Extension to Cellular calls for all internally originated calls. External call filtering does the same for all public network incoming calls.

When call filtering blocks a call, the cell phone does not receive the Extension to Cellular call. If so, the call can then be forwarded, or coverage treatment can be applied.

Call filtering only applies to Extension to Cellular calls extended to the cell phone; calls to the desk set are unaffected. If not answered, the call will go to the coverage path.

Caller ID from the cell phone

If administered with Origination Mapping, the Extension to Cellular telephone gains the identity of the user's office extension when calling into the Communication Manager. Origination mapping means that the cell phone is administered to present the office caller ID. When the cell phone user calls into the office, the person receiving the call sees the office name and office number of the caller, not the cell phone caller ID. This type of administration provides in-house caller identification at the destination telephone because the cell phone is mapped to the office telephone.

An Extension to Cellular telephone that is administered to gain the identity of the office telephone has the following functionality:

- When calling a number at the office (Communication Manager), the destination telephone displays the name and extension as the caller ID.
- A user can initiate a call to the office on an Extension to Cellular cell phone and pick up that same call in progress on the office telephone.
- When calling into the same office switch on which Extension to Cellular is administered, the Extension to Cellular cell phone functions as if it were an office telephone extension. For example, a corporate voice messaging system receives an Extension to Cellular cell phone call; the system recognizes the call as an extension on the switch.
- Origination mapping allows feature invocation by Feature Name Extension (FNE).

In some parts of the world, the calling number from a cellular phone may or may exclude the country code. With origination mapping, you can map a calling number to a station regardless of whether the calling party number contains a country code.

To display an incoming international call on an endpoint, prefix the calling number with the international access code. The International Access Code field is associated with the location of the trunk on which the calling number arrives. To prefix the calling number with the international access code, go to the Locations Parameter screen and administer the International Access Code field. If the International Access Code field is blank, Communication Manager fetches the international CPN prefix from the Feature Related System Parameter screen and prefixes the CPN code to the calling party number.

If the existing administrator option, Passed Prefixed CPN: ASAI, is set on the Feature Related System Parameter screen, the ASAI displays the calling party number with the International CPN prefix. If the existing administrator option, Passed Prefixed CPN: ASAI, is not set, the ASAI displays the calling party number without the International CPN prefix.

To handle calling numbers with country codes, enter the country code (CC) in the **CC** field on the Off-PBX Station Mapping screen. Communication Manager will match the calling number either with or without its country code with the office extension.

Capacity limitations for Extension to Cellular

Extension to Cellular applications are allocated on a per station basis.

Note:

Use traffic engineering to ensure that there are enough trunks available to handle the traffic sent to the cell phones.

Extension to Cellular impacts trunk utilization extensively if a large percentage of the switch users are *Extension to Cellular* users. In many cases, the outbound trunk calls might not actually complete since the user can answer at the *Extension to Cellular* station.

The number of simultaneous call terminations towards the off-PBX station is limited to the maximum number of call appearances for each extension on the switch. However, this call limit number is usually less than the maximum call appearances. For example, Extension to Cellular users normally want the call limit at two, since most cell phones can handle only two calls at a time.

Extension to Cellular Configuration sets

A configuration set defines several call treatment options for Extension to Cellular cell phone calls. Extension to Cellular administration supports up to 99 configuration sets. All configuration sets begin populated in the system using default values. Because there are 99 configuration sets available, multiple combinations of the options can be administered, thus accommodating requirements for many cellular service providers.

For more information, see Changing configuration sets.

Related links

Changing configuration sets for Extension to Cellular on page 785

Extension to Cellular Feature Access Codes

A user can activate Communication Manager features related to Extension to Cellular through telecommuter Feature Access Codes (FACs). A user can access an FAC by one of these methods:

- Dialing the telecommuter number
- Dialing the remote access number
- Dialing the idle appearance select FNE

The EC500 DTMF feature access code detection during a call works only when SIP and H323 signaling is used for the EC500 call leg. You must set the DTMF detection mode of the EC500 signaling group to **rtp-payload** or **out-of-band**.

The FACs require the entry of a station extension and Station Security Code. For more information about Extension to Cellular Feature access codes, see the *Avaya Extension to Cellular User's Guide*, 210-100-700.

EC500 Activation/Deactivation

The Enhanced EC500 Activation Feature Access Code enables the delivery of calls to the cell phone when the associated office telephone receives a call. It applies to the EC500 and PBFMC applications (all other applications are always enabled).

The Enhanced EC500 Deactivation Feature Access Code disables the delivery of calls to the cell phone when the associated office telephone receives a call. It applies to the EC500 and PBFMC applications (all others applications are always enabled and are unaffected by this feature).

For more information, see Creating FACs to enable/disable Extension to Cellular.

Related links

Creating FACs to enable/disable Extension to Cellular on page 778

Self Administration Feature Access Code

The Self Administration Feature Access Code for EC500 (SAFE) can be altered by a user to change to the **dial prefix**, **CC** (country code), and **phone number** fields of the station-mapping form. This feature can be used for Extension to Cellular, Cellular Service Provider (CSP), Service Provider Fixed-Mobile Convergence (SPFMC), and Public Fixed Mobility (PBFMC) applications.

With SAFE, you can administer the **dial prefix** and the **country code** fields and the telephone number. Enhanced SAFE uses the asterisk (*) as the field delimiter between the dial prefix, the country code, and the phone number fields. SAFE also recognizes the sequence "**#" as meaning remove existing entries in the field (**dial prefix**, **country code**, and **phone number**).

Using the SAFE Access Code, users can self-administer cell phone numbers for use with Extension to Cellular. The user calls one of up to four SAFE access codes and enters the cell phone number to add or change. SAFE automatically enables Extension to Cellular, and the cell phone number is recorded in the Stations with Off-PBX Telephone Integration screen (**`change off-pbx telephone station-mapping`**) on the **Phone Number** field.

The administration sequence for the user differs based on what phone is used to access SAFE. See the *Avaya Extension to Cellular User's Guide*, 210-100-700 for more information.

You cannot enter a destination number through SAFE if a user's desk set is restricted from calling that number.

For more information, see Creating a Self Administration Feature access code.

Related links

Creating a Self Administration Feature access code on page 776

Conditional Call Extending

With the Conditional Call Extending feature, you can limit the type of calls that are extended to the cell phone when EC500 is enabled. You can administer the Conditional Call Extending settings and apply these settings to a specific application instead of the station as a whole. User can also set the Conditional Call Extending settings. Conditional Call Extending feature is used by the SIP and FMC applications such as PBFMC, PVFMC, and SPFMC. With the Conditional Call Extending feature, you can reduce the cellular use by restricting the unrequired calls which results in improved productivity.

You can use the Conditional Call Extend Enable FNE and the Conditional Call Extend Disable FNE to enable and disable conditional call extending settings. To do that, you can use the Conditional Call Extend Activation FAC and the Conditional Call Extend Deactivation FAC.

You cannot administer the Conditional Call Extending state on the users' stations. User cannot make all Conditional Call Extending setting changes. User can administer the Conditional Call Extend FNEs or FACs on the station. To activate the Conditional Call Extending settings, you must enable the EC500 state for the user's station. Conditional Call Extending settings do not work when you disable the EC500 state.

You can set six different independent settings to decide the type of call to extend:

1. Standard calls to the station
2. Calls covered or forwarded to the station
3. Calls to the station through a hunt group
4. Intercom calls to the station
5. Priority calls to the station
6. Calls restricted by a COR permission matrix

For more information, see Administering Conditional Call Extending for Extension to Cellular

Related links

Administering Conditional Call Extending for Extension to Cellular on page 787

Feature buttons on the office telephone

You can enable Extension to Cellular applications with office telephone feature buttons. For example, you can administer feature buttons for enabling and disabling Extension to Cellular. You can also administer an optional timer for Extension to Cellular through the enable and disable feature button for H.323 and DCP phones. The Extension to Cellular feature button is available on telephones that support administrable feature buttons. With the Extend Call feature button, users can answer an Extension to Cellular call on the office telephone, and then move the call seamlessly to the cell phone.

The feature button will not enable or disable Extension to Cellular when a cellular service provider (CSP) or Service Provider Fixed-Mobile Convergence (SPFMC), application provides the Extension to Cellular capability.

The extend call button is available on wired office telephones. It is used to add the cell phone to an existing call at the office telephone.

For more information, see Administering a feature button to extend a call.

Related links

Administering the extnd-call feature button through SAT on page 780

Feature Name Extensions with Extension to Cellular

When the Extension to Cellular feature is enabled, a mobile phone user can activate certain Communication Manager features by dialing a Feature Name Extension (FNE). Each FNE requires a direct inward dialing (DID) number. You must create the FNEs that comply with the dial plan administered systemwide.

With the Additional Security for an EC500/One-X Mobile Lite call (AEFSC) feature, when a user makes an FNE call from a mobile phone, the system authenticates the call with the station security code (SSC). Communication Manager provides a high-pitched tone to prompt the user to enter the SSC. The call fails without a valid SSC.

When a user wants to make an EC500 call, the caller must dial the SSC after the FNE number. For example, <FNE> [Dial tone] <SSC> # [Dial tone or confirmation tone] <Subsequent digit or extension> #. If a caller wants to activate or deactivate a feature using FNE, the caller must dial SSC after the FNE number. For example, <FNE> [Dial tone] <SSC> # [Confirmation tone or error tone].

For more information, see *Setting up Feature Name Extensions set*.

Related links

Setting up Feature Name Extensions set on page 776

Multiple sets of Feature Name Extensions with Extension to Cellular

You can use the Communication Manager to gain multi-country switch access by administering multiple sets of Feature Name Extensions (FNEs). You can have one Communication Manager with different gateways in multiple locations. Each gateway can have its own FNE set. The FNE sets are administered on the Off-Pbx-Telephone Feature-Name-Extensions screen. Each FNE is administered on its own form. For example, you can have one Communication Manager with gateways in France, Poland and Germany. The user can use the FNEs on the gateways closest to the user’s physical location. If the user is in France and has to conference a call, the user can use the FNE on the gateway in France. In this way, you can reduce long distance charges by choosing a gateway that can most optimally process the call.

Mobile Call (CTI) Extension

Using this feature, a CTI application can control extending of calls to Single and Dual mode applications: EC500, CSP, SPFMC, PBFMC, and PVFMC. If multiple applications are administered for an endpoint, the desk set applies the MCE only to the supported applications.

The feature is invoked by making the office telephone call the Mobile Call Extension. This causes a call to be initiated to the phone number of the application. This extension is administered on the Off-Pbx Mobile-Feature-Ext screen.

When the call is answered, any FNE-based operation can be applied to the call, such as, recall, conference or transfer. After the conference or transfer, the cell phone call remains an OPTIM call associated with the calling station.

The user receives intercept tone for invalid calls to the Mobile Call Feature Extension, such as a call initiated from off the switch, or from a desk set that does not have a supported OPTIM application administered.

Multiple applications with Extension to Cellular

You can administer up to four Extended Access applications on one telephone. Extended Access applications include Extension to Cellular, Cellular Service Provider (CSP), Service Provider Fixed-Mobile Convergence (SPFMC), SIP, and Public Fixed Mobility (PBFMC) PBFMC and Private Fixed Mobility PVFMC. You can also administer more than one instance of an application on one telephone. For example, you can map one office telephone to two different cell phones through Extension to Cellular.

When you map an office telephone to multiple applications, any Communication Manager feature enabled on one endpoint, such as the cell phone, applies to all other endpoints.

The **EC500 status** button shows a single station-wide state of EC500 activation regardless of the number of applications administered.

The **Extend Call** button extends an active call to all mapped endpoints.

Extend call FNU is invoked at a mobile SIP endpoint or an OPS SIP station and extends an active call to all mapped mobile endpoints. The Extend Call FNU when invoked at an OPS SIP station or a mobile SIP endpoint will not extend the call back to itself.

Bridging tone applies when a call is active and a user on another mapped endpoint attempts to bridge on to the call. The following occurs:

- If a cell phone bridges to desk set on an active call – no tone will be heard.
- If the desk phone user attempts to bridge on a call that is active on cell phone - the cell phone user will hear intrusion tone.
- If the SIP OPS desk phone user attempts to bridge on a call that is active on cell phone - the cell phone user will hear intrusion tone.
- If a cell phone bridges to SIP OPS desk phone on an active call – the cell phone user will hear intrusion tone.
- If desk phone user attempts to bridge on a call that is active on a SIP OPS desk phone - the SIP OPS phone user will hear intrusion tone.
- If a SIP OPS desk phone user attempts to bridge on a call that is active on desk phone - no tone will be heard.

Using Self Administration FAC for EC500, a user can self-administer a cell phone number on the **phone number** field of the off-PBX telephone station-mapping screen for the EC500 and CSP applications. SAFE only applies to EC500, CSP, SPFMC, and PBFMC.

Exclusion will apply to all mapped endpoints; they will be excluded from an active call other than the endpoint that invoked exclusion.

All features invoked at any OPTIM endpoint will apply to all other endpoints. For example, SAC will apply to all mapped endpoint regardless of which one invoked SAC.

Using multiple applications or single applications, only one origination-mapping per phone number can be used whereby the same cell phone number cannot be administered more than once as both or origination.

Support for Avaya one-X® Client Enablement Services

Communication Manager uses Avaya one-X® Client Enablement Services (formerly known as Avaya one-X® Server) to configure and control a set of Communication Manager features. Client Enablement Services control alerting of any off-PBX telephones, on-PBX telephones, and the desk set by indicating which particular phone rings when a call is received. Each extension can support four one-X applications. The Client Enablement Services can extract information from Communication Manager. A SIP subscription is used as a transport mechanism between Client Enablement Services and Communication Manager. The SIP trunk is used for signaling and cannot be used to send voice traffic. The application data is passed in the message bodies of the Subscribe, Notify, and associated Response messages.

Communication Manager Release 7.0 and later supports 20 Client Enablement Services servers.

Note:

On-PBX phones require version 6.2 of Client Enablement Services.

You can use Class of Restriction (COR) to control the stations that have Client Enablement Services support. You can see the control status of a station using the **`status station`** command.

The Client Enablement Services feature provides a way to control ringing of multiple phones tied to one extension and to provide real time calling information for a synchronized call log. Each Client Enablement Services subscribe to one or more event packages.

The avaya-cm-one-x-call event package is used to convey control information from Client Enablement Services and the status information from Communication Manager. The avaya-cm-one-x-config event package conveys configuration information to a mobile client. The avaya-cm-one-x-call package conveys information in the bodies of SIP Subscribe, Notify, and Response messages. The message information is in XML format. Communication Manager provides administrative capabilities for Client Enablement Services feature. The Client Enablement Services feature supports the following:

Static Call Handling	By using this feature, the server can provide phone numbers from one mobile phone and maximum 3 off-PBX or on-PBX telephones. The server can control alerting of any off-PBX telephones, on-PBX telephones, and desk sets. By using the Static Call Handling feature, the server indicates whether a particular phone must ring or not when an incoming call is received. A static mapping is used when a trigger mapping fails due to loss of connectivity between Communication Manager and Client Enablement Services.
Triggered Call Handling	When this option is active, an incoming call does not alert a desk set or an off-PBX or on-PBX telephone. Communication Manager contacts Client Enablement Services with substantial information to apply pre-screening rules to each incoming call. Client Enablement Services responds to Communication Manager with a list of the phone numbers to alert. The phone numbers can be any combination of a desk set extension, one mobile phone, and maximum 3 other off-PBX or on-PBX phone numbers.
Call Progress Reporting	Client Enablement Services uses this feature to receive a report on calls to and from a station with the one-X application. The report is generated when a station: • initiates an outbound call • receives a call • answers a call • ends a call **Note:** The report generated is not a Call detail Recording (CDR) report.
Extended Access	The off-PBX telephones use this feature to invoke a subset of Communication Manager features by dialing a DID number. These numbers are then converted in to Feature Name Extensions. **Note:** Extended access is inapplicable for the on-PBX telephones. The on-PBX telephones invoke features directly by activating relevant feature buttons or by dialing the Feature Access codes.
Autonomous Operation	Autonomous operation occurs when there is a loss of communications between one-X server and Communication Manager. During autonomous operation, Call Handling is active and Triggered Call Handling and Call progress Reporting are inactive. The Static Call Handling profile is used when the Triggered Call Handling fails. When no Static Call Handling profile exists, an incoming call alerts only the desk set.

To ring an on-PBX destination extension, call routing is determined by the following rules:

- Any extension that represents a group (for example, hunt group.) is not routed.
- An extension that is under One-X control is routed, but none of the one-X destinations for that extension is routed.
- An extension that has any OPTIM application is routed, but none of the one-X application numbers for that extension are routed.

Note:

The Off-premises station (OPS) SIP phone is also routed.

- An extension that has any form of call-forwarding or coverage or circular station hunting is routed directly to that extension and ignores the forwarding or coverage or hunting treatment for that extension.
- Bridged appearances of the on-PBX destination extension are not notified.
- Call pickup groups or team button members with on-PBX destination extension are not notified about a ringing call, and are unable to pickup that calls.
- Intercom calls are routed, but not with any automatic answer if enabled.

For more information, see *Administration for Avaya one-X® Client Enablement Services*.

Related links

Administration for Avaya one-X Client Enablement Services on page 788

R2MFC trunks with Extension to Cellular

OPTIM applications available with a Single mode license support calls over high function digital Multi Frequency Compelled (MFC) Signaling trunks. The digital MFC trunks provide answer supervision and can transmit calling number information. MFC trunks are supported only if answer supervision information is provided.

To get efficient digit processing, the administrator can insert 9 (or equivalent ARS or AAR Access Code) to use the digit conversion table which is administered on the ARS Digit Conversion screen. The **ANI Reqd** field indicates whether ANI must be requested for MFC trunk. This field has to be set for Extension to Cellular origination features to work.

The MFC trunks support the following features:

- Origination mapping
- Termination mapping
- SAFE
- FNEs
- Configurations Set Options
  - Calling Number Style
  - CDR for Calls to EC500 Destination
  - CDR for origination
  - Cellular voice mail avoidance
  - Barge-in tone

Security features for Extension to Cellular

Extension to Cellular security features include security codes and security tones.

Security codes for Extension to Cellular

Station security codes (SSC) provide security to station users by preventing other users from accessing functions associated with a station. Security codes are used with remote activation of Extension to Cellular. With Remote activation, off-premises users can dial in to Communication Manager using a special DID number, that maps to a Remote Access Extension number. Users can then enter the security code, and can use any feature that can be accessed through Feature Access Codes. SAFE requires SSCs. Conditional Call Extending also requires SSC.

However, security codes are not always necessary for Extension to Cellular activation or deactivation.

- If the user's Class of Service provides console permissions, then a SSC is not needed.
- Users do not need a security code if the enable/disable Extension to Cellular button is administered on the office telephone.
- Enabling/disabling Extension to Cellular through an FNE used on a mapped cell phone does not require a Station Security Code.

As administrator, you can create a system-wide SSC change Feature Access Code (FAC) that users can invoke to change their desk phone's SSC. You must also administer and provide specific SSCs to users. A user cannot change a blank SSC. An SSC can be administered for an AWOH station.

With the Extension to Cellular feature, users can enable or disable all mapped extensions at one time, using the Station Security Code for the office telephone.

Security tones for Extension to Cellular

The Conference and Barge-in tones provide more security for Extension to Cellular calls. During an Extension to Cellular call, a user hears a tone when the user picks up the office telephone that is mapped to the mobile phone.

When an office telephone is mapped to multiple applications, the Barge-join tone is played when a user bridges on to a call through a telephone mapped to the office telephone. The Barge-in tone is played only when the user uses the deskphone to bridge on to the call answered on Extension to Cellular device. The tone is played to all users connected on a call.

If additional security is required, administer one of the exclusion features. When you enable exclusion on a telephone, the security feature applies to all off-PBX applications on the telephone.

If the Additional Security for an EC500/One-X Mobile Lite call feature is administered, when a user makes an FNE call from a mobile phone, the system authenticates the call with the station security code (SSC).Communication Manager provides a high-pitched tone to prompt the user to enter the station security code. The call fails without a valid SSC.

Shared Voice Connections with Extension to Cellular

In the Shared Voice Connections feature, you can share a single trunk for multiple calls as follows:

The user makes a call that is connected to the Communication Manager and they make another very short call (dialing an FNE) to put that call on hold. The connection between the cell phone

and the Communication Manager is still active and can be used to dial another call. In this way one connection between the cell phone and the Communication Manager is used to manage two phone calls.

Any time you initiate or answer the second cell phone call, the first call is put on hold at the PBX and its voice connection is dropped; it is combined with the new active call as a shared connection. You can use shared voice connection option only with the FMC applications such as PBFMC, PVFMC, and SPFMC.

You can use the Recall FNE, Conference Complete FNE, and Transfer Complete FNE with the shared voice connection feature as follows:

- When you have a shared connection having an active voice call and a held call you can dial the Recall FNE to put the active call on hold and connect to the previously held call.
- You can use the Conference Complete FNE or the Transfer Complete FNE when there is an active call and a held call in a shared connection. The Conference Complete FNE conferences the two voice calls together while the Transfer Complete FNE transfers the held call to the active voice call.

  Note:

  If the long hold recall timer is administered, then you do not need to use the Recall FNE. The held call will be connected as soon as the long hold recall timer is expired and the active call will be placed on hold at office telephone.
- With the PVFMC application you need not use the Shared Voice Connection feature since SIP supports signaling hold, transfer, and conference.
- When your OPTIM application is part of one shared voice connection, you cannot be part of any other shared voice connection. You can use the same call appearance in multiple shared voice connection when the connections are associated with different OPTIM applications.

When you establish a shared connection, additional calls initiated or answered by the cell phone do not have any effect on the existing calls. When the active voice calls drops and only held call is there, then the shared connection becomes a residual shared connection. When the cell phone initiates or answers a new call, then the new call is added to the residual shared connection to form a shared connection. You can use the Held Appearance Select FNE to connect to the held call in a residual shared connection.

Sharing Mappings among Communication Manager PBXs with Extension to Cellular

With the Sharing Mapping among Communication Manager PBXs feature, you can share the station name and station mapping information among multiple Communication Manager using SIP subscriptions. Extension to Cellular users can be recognized on another PBX where they are not administered. When the foreign Communication Manager acquires the shared information, it creates a temporary mapping to associate the shared cell phone number with the shared extension and the station name. Any calls with a calling number matching a temporary mapping can use the shared station name and extension for incoming call displays.

A SIP signaling group is needed for each pair of Communication Manager that share mappings. No SIP trunk group is required. Up to three such pairs may be administered allowing up to four Communication Manager to shared mappings.

For more information, see Administering Sharing Mapping among Communication Manager PBXs.

Related links

Administering Sharing Mapping among Communication Manager PBXs for Extension to Cellular on page 788

SPFMC OPTIM Application overview

Service Provider Fixed-Mobile Convergence (SPFMC) is similar to the Cellular Service Provider (CSP) application, but for service providers that support dual mode phones. SPFMC is always enabled and can handle anonymous SIP calls by blocking the caller's identity. SPFMC ignores the EC500 state of a station.

An SPFMC application can be associated with a PVFMC application to support a dual-mode cell phone. You can define the application to be part of a dual-mode pair. There may be two sets of dual-mode pairs. A **Dual Mode** field on the station mapping screen indicates which application is part of a dual-mode pair. **Dual Mode** field can have three values: dm1, dm2, or blank. If **Dual Mode** field is blank then application is not part of a dual-mode pair. Only FMC applications can have a non blank value in the **Dual Mode** field. The values of dm1 and dm2 indicate if the application belongs to a dual-mode pair. There can be two sets of dual-mode pairs (two dual mode phones) mapped to a desk set.

Using desk phones and Extension to Cellular phones with MOC

The integration of Microsoft Office Communicator (MOC) with Communication Manager through ASAI supports bridging; that is, having two user functions simultaneously. For example, you can simultaneously attend two calls: an active call on a desk phone and an active call on an off-PBX destination, such as a mobile phone. To integrate MOC with Communication Manager, set the **MOC Control** field to y on the Class of Service form. The off-PBX Telephony Integration and Mobility (OPTIM) applications, such as CSP, EC500, PBFMC, SPFMC, and Avaya one-X® Client Enablement Services, support this feature.

The bridging feature applies to the following scenarios:

- When you are on a desk phone call and answering an incoming business call on your mobile phone simultaneously, without placing the desk phone call on hold
- When you are on a business call on your mobile phone and you pick up the desk phone to dial a number or receive a call

The MOC client does not officially support bridging. You cannot appear to be active on the desk phone and your mobile phone simultaneously. Therefore, one of the active calls always appears to be on hold to the MOC client. However, when you register the MOC client, the call on the off-PBX phone appears to be on hold to the MOC client and the desk phone. However, you can still talk on both the off-PBX phone and the desk phone. To register the MOC client, go to the Class of Service screen and enable the **MOC Control** field.

When you disconnect the call on the mobile phone, the system disconnects the call from the mobile phone and the desk phone. However, if you bridge the same call to the mobile phone from the desk phone, you must manually disconnect the call from the mobile phone and the desk phone.

Note:

Avaya recommends that MOC must be the only ASAI application registered to control the supported stations.

Telephones supported by Extension to Cellular

The following telephone types can be administered as the office telephone for Extension to Cellular:

2402	4601	4610	4621	4625	6402	6408+	6416D+
2410	4602	4612	4622	4626	6402D	6408D	6424D+
2420	4606	4620	4624	4630	6408	6408D+	1603
1608	16CC	9620	9630	9640	9650	1408	1416
1608	1616	8403B	8405D+	8410D	8411B	8411D	8434D
9620SIP	9630SIP	9640SIP	9650SIP	9608	9611	9621	9641
9608SIP	9611SIP	9621SIP	9641SIP	9608SIPCC (“ops” application only)	9611SIPCC (“ops” application only)	9621SIPCC (“ops” application only)	9641SIPCC (“ops” application only)
Avaya J129 IP Phone	Avaya J169 IP Phone	Avaya J179 IP Phone	J169CC	J179CC	AvyaSIP	AvyaSIPCC	-

Note:

- Telephone type XMOBILE is not listed in the table. Endpoints configured as XMOBILE cannot access important enhancements to EC500, such as support for SIP trunk groups. For information about converting from an XMOBILE configuration to the officially supported EC500 configuration, see the *Extension to Cellular upgrades from prior versions* section later in this chapter.
- Prior to Communication Manager Release 10.2, J139, J159, and J189 must be aliased. The J139 IP Phone should be administered as J169 IP Phone. The J159 IP Phone should be administered as a J169 IP Phone with single expansion module, and the J189 IP Phone should be administered as a J179 IP Phone with at least one expansion module. If a JEM is attached, J189 IP Phone will be administered as a J179 IP Phone with two or more expansion modules. With Communication Manager Release 10.2, the J139, J159, J189, and J189CC endpoints will appear as AvyaSIP or AvyaSIPCC type set. You must administer these endpoints in System Manager. When you add these endpoints from System Manager, Communication Manager only display these endpoints.

Voice mail with Extension to Cellular

Because the cell phone is treated as a local extension on the Avaya server running Communication Manager, the telephone can be completely integrated with the corporate voice messaging system. However, the cell phone can also keep the cellular service provider voice mail. This dual messaging capability presents an issue of where a user wants the message to go: corporate voice mail or cellular voice mail.

With regards to voice mail functionality and Extension to Cellular:

- The office number retains the primary extension on the Avaya server running Communication Manager.
- Calls to the office number simultaneously ring the office number and the cell phone. If neither answers, standard coverage arrangements take effect.
- As needed, you can disable Extension to Cellular when not in use to ensure that all unanswered calls go to the corporate voice messaging system.

The system administrator can control in-service and out-of-service status of the mapped extensions through a busy out and release maintenance capability. An unanswered call either ends at the corporate voice mail system or at the cellular service provider (CSP) voice mail system. The amount of control over the terminating voice mail system is limited. As administrator, you can use Cellular Voice Mail Avoidance and ring timing to direct Extension to Cellular calls to the appropriate voice mail coverage. See also, Cellular Voice Mail Avoidance Using Confirmed Answer.

Voice Mail Avoidance with Extension to Cellular

Communication Manager Extended Access Cellular Voice Mail Avoidance reduces the uncertainty as to where unanswered calls to the cell phone go for coverage. An unanswered call typically either ends at the corporate voice mail system or at the cellular service provider (CSP) voice mail system. You have limited control over the terminating voice mail system. You can administrator the number of ring cycles before a call goes to the corporate and cellular voice mail systems and enable Cellular Voice Mail Avoidance through Communication Manager.

The cellular voice mail system can lead to several problems for the user. The cellular network routes calls to cellular voice mail when any of the following conditions exist:

- Users do not answer a ringing call.
- The cell phone is in a bad coverage area.
- The cell phone is turned off.

With Cellular Voice Mail Avoidance, Communication Manager detects when the cell phone is not the entity answering the call and the call goes to Cellular Voice Mail. Communication Manager then “brings the call back” so that the call follows normal coverage treatment. The office telephone rings an appropriate number of times before sending the call to coverage.

Use timing to route calls with Extension to Cellular

Unanswered office telephone calls are usually routed to a corporate voice messaging system after a predetermined number of rings. Similarly, most cellular service providers allow customers to route unanswered calls after a specified number of rings.

The number of times the desk phone or cell phone rings can be manipulated to help direct a call to the system of choice. To only receive voice messages through the corporate voice messaging system set the voice mail feature on the cell phone to a higher number of unanswered rings than the corporate system. For example, say the corporate voice messaging system automatically picks up an unanswered call on the third ring. The user then sets the cell phone voice mail system to pick up unanswered calls on the fourth or fifth ring.

Timing cannot ensure which voice mail system covers an unanswered call.

Users who cannot adjust the number of rings on the cell phones must contact the cellular service provider for assistance.

See also, Cellular Voice Mail Avoidance Using Confirmed Answer.

Prevent coverage by cellular voice mail

Most cellular service providers route calls automatically to the cellular voice mail system when a cell phone is turned off or in an out-of-coverage area. To prevent work-related calls from being automatically routed to a cellular voice mail system, tell users to disable Extension to Cellular before shutting down the cell phone. Then, the corporate voice messaging system covers incoming calls to the office number and the cellular voice mail system picks up personal calls.

Note:

If a cell phone is used exclusively for business purposes, users can request that the cellular service provider disable voice mail.

See also, Cellular Voice Mail Avoidance Using Confirmed Answer.

Cellular Voice Mail Avoidance Using Confirmed Answer

The Communication Manager supports the Confirmed Answer option for cellular voice mail avoidance for any OPTIM application, including Extension to Cellular. With Confirmed Answer set to yes on the user's Configuration Set screen, when answering the phone, the user hears the dial tone. The user must then press one of the digits on the cellular phone's keypad. Until the system receives a digit, the system does not treat the call as answered. The time to wait for the digit can be administered from 5-20 seconds, with a default of 10 seconds. Communication Manager plays recall dial-tone to indicate that input is expected. During the response interval, the original call continues to alert at the desk set and any stations bridged to the call. If a user does not enter a digit before the time-out interval expires, the call is pulled back from the cell phone.

If the user wants to use the cell phone for both personal and business calls, the Confirmed Answer option can be used to both guarantee that business calls (to the enterprise phone number) do

not end up in cellular voice mail. The Confirmed Answer option also notifies the user on answer whether the call went to the enterprise phone number, or directly to the cell phone number.

- In some businesses with the Extension to Cellular (such as for after hours support), it is critical that a call be treated as answered only if a person answers the call. In such a scenario, Confirmed Answer is the only reliable voice mail avoidance method.
- Confirmed Answer is the most reliable form of cellular voice mail avoidance. An added benefit of the feature is that the dial-tone is a signal to the user that the call is a business call, not a personal call.

See also, Setting up a Cellular Voice Mail Avoidance timer.

Extension to Cellular administration

The following steps are part of the administration process for the Extension to Cellular feature:

- Mapping an office telephone to a cell phone
- Setting up Feature Access Codes
- Creating a telecommuting access number
- Setting up Feature Name Extensions set
- Creating a Self Administration Feature access code
- Administer the office extension
- Administer the Feature Access Code
- Creating FACs to enable/disable Extension to Cellular
- Creating a Station Security Code Change FAC
- Creating a system-wide SSC change FAC
- Defining the Station Security Code length
- Administering an enable/disable feature button
- Changing the EC500 state on the station form
- Administering a feature button to extend a call
- Setting the optional timer
- Reviewing feature button assignments
- Sending 10-digit caller identification for locally originated calls
- Administering call filtering
- Administering voice mail coverage
- Setting up a Cellular Voice Mail Avoidance timer

- Using timing to route calls to voice mail
- Setting up Call Detail Recording
- Enable CDR for the outgoing trunk
- Enabling CDR for Extension to Cellular
- Generating two CDR records
- Changing configuration sets
- Administering the barge-in tone
- Displaying System Capacity
- Setting up One-X Server integration

Related links

Mapping an office telephone to a cell phone on page 774
Setting up Feature Access Codes for Extension to Cellular on page 775
Creating a telecommuting access number on page 776
Setting up Feature Name Extensions set on page 776
Creating a Self Administration Feature access code on page 776
Creating FACs to enable/disable Extension to Cellular on page 778
Creating a Station Security Code FAC on page 778
Administering an Extension to Cellular enable/disable feature button on page 779
Administering the extnd-call feature button through SAT on page 780
Reviewing Extension to Cellular feature button assignments on page 781
Viewing the button labels for the feature buttons on page 781
Sending 10-digit caller identification for locally originated calls on page 781
Administering Confirmed Answer for Cellular Voice Mail Avoidance on page 782
Administering call filtering for Extension to Cellular on page 782
Administering voice mail coverage for Extension to Cellular on page 782
Setting up Call Detail Recording for Extension to Cellular on page 783
Changing configuration sets for Extension to Cellular on page 785
Administering the barge-in tone for Extension to Cellular on page 786
Displaying System Capacity for Extension to Cellular on page 787
Administering Conditional Call Extending for Extension to Cellular on page 787
Administering Sharing Mapping among Communication Manager PBXs for Extension to Cellular on page 788
Administration for Avaya one-X Client Enablement Services on page 788
Setting up One-X Server integration on page 789

Preparing to administer Extension to Cellular

Procedure

1. Prepare a plan of numbers and codes for Extension to Cellular users. For more information, see Extension and codes plan on page 772.

2. Verify optional customer features required for Extension to Cellular.

Extension and codes plan

The extension and codes plan for Extension to Cellular users includes the following numbers and codes:

- the Station security code associated with the office number
- the Station Security Code Change Access Code
- the EC500 Self Administration Access Code
- the Extension to Cellular disable and the Extension to Cellular enable feature access codes
- the Avaya Extension to Cellular telecommuting access number
- a list of all the Feature Name Extensions (FNEs) that you set up and the features that the FNEs are mapped to

Reviewing customer options

Procedure

1. Enter `display system-parameters customer-options`.
2. On page 1 of the Optional Features screen, ensure that:
   a. The **G3 Version** field shows V14 or later.
   b. The **Maximum Off-PBX Telephones - EC500** field shows the number of licenses purchased for Extension to Cellular and the number of licenses purchased for SMODE.
   c. The **Maximum Off-PBX Telephones - PBFMC** field shows the number of licenses purchased for DMODE.
   d. The **Maximum Off-PBX Telephones - PVFMC** field shows the number of licenses purchased for DMODE.
3. On page 2 of the Optional Features screen:
   - For H.323 trunks, ensure that the **Maximum Administered H.323 Trunks** field shows a value greater than zero.
   - For SIP trunks, ensure that the **Maximum Administered SIP Trunks** field shows a value greater than zero.
4. On page 3 of the Optional Features screen, ensure that the **ARS** field shows y.
5. On page 3 of the Optional Features screen, ensure that:
   - the **Enhanced EC500** field shows y.

     If the **Enhanced EC500** field shows y, the screens that are tied to the **`off-pbx-telephone`** commands become available.
   - the **ISDN-BRI Trunks** field, the **ISDN-PRI** field, the **Multifrequency Signaling** field, or all three fields show y.

- for H.323 and SIP stations, the **IP Trunks** field shows y.
- the **Extended Cvg/Fwd Admin** field shows y.

  With this setting, you can get access to the Telecommuting Access screen and set the **Telecommuting Access Extension** field. After you set this field, users can dial the telecommuting access extension from their EC500-enabled cell phones, hear the dial tone and then dial the feature access codes after the dial tone.

6. Click `Enter` to exit the screen.

   For more information on the Optional Features screen, see *Avaya Aura® Communication Manager Screen Reference*.

Screens for administering Extension to Cellular

Screen name	Purpose	Fields
Stations with Off-PBX Telephone Integration	Map station extensions to application types and external telephone numbers.	All
Off-PBX Telephone Mobile-Feature- Ext	Administer CTI feature	Mobile Call (CTI) Extension
Feature Access Code (FAC)	Set up access codes for Communication Manager features	Feature Access Code
Extension to Call Which Activate Features by Name	Map a dialed extension to activate a feature (FNE) within Communication Manager from a cell phone. Some FNEs require FAC administration.	Extension
Telecommuting Access	Create an Extension to Cellular remote access number	All
Security-Related System Parameters	Define a system-wide Station Security Code length	Minimum Station Security Code Length
Station	Assign feature buttons and timers **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

Table continues…

Screen name	Purpose	Fields
Coverage Path	Set up number of unanswered rings before coverage	Number of Rings
Trunk Group	Enable Call Detail Recording for outgoing trunk	CDR Reports
DS1 Media Module	Administer a DS1 media module for R2MFC for Extension to Cellular use.	Signaling Mode: CAS Interconnect: CO
Trunk Group	Administer a DID trunk group for R2MFC signaling and Extension to Cellular use.	Group Type: did Trunk Type: immed-start Incoming Dial Type: mf (for MFC signaling)
Trunk Group	Administer a DOID trunk group for R2MFC signaling and Extension to Cellular use.	Group Type: diod Trunk Type: immed-start Trunk Type: immed-start Outgoing Dial Type: mf (for MFC signaling) Incoming Dial Type: mf (for MFC signaling) Receive Answer Supervision? y
Multifrequency- signaling-related- parameters	Administer MFC parameters needed for Extension to Cellular.	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

Mapping an office telephone to a cell phone

Procedure

1. Enter `add off-pbx-telephone station-mapping`.
2. Fill in the information in all fields for each Station Extension.

   You can add up to sixteen associations between an office telephone and an external telephone. You can add up to four associations for the same extension.
3. Page down to the second page of the Stations with Off-PBX Telephone Integration screen.

The second page displays the information that you have entered in the **Station Extension** field on the first page as read-only information.

4. Enter the Mapping Mode for each Station Extension.
5. Enter the category of Calls Allowed for each Station Extension.
6. Enter the type of Bridged Calls allowed.
7. Tab over to the **Location** field.

   Enter the Location value for each OPS, PBFMC or PVFMC application that you have administered on Page 1.You can find the location value on the Locations screen (**`change locations`**).

   If you need the cellular phone to have the same location as the corresponding desk phone, and the user's desk phone is a:

   - Non-IP set, enter the location of the desk phone's gateway.
   - IP set, enter the location of the network region for the desk phone.

   If the location field on the Station screen is left blank, Communication Manager uses the location of the incoming trunk.
8. Page down to next page, Stations with Off-PBX Telephone Integration, page 3.
9. For Sharing Mappings among Communication Manager PBXs feature, enter the Share Level value for EC500, CSP, PBFMC, and SPFMC applications (See Administering Sharing Mapping among Communication Manager PBXs).
10. For Conditional Call Extending feature, enter `Calls Accepted S C H I P R` and `COR` field values (See Administering Conditional Call Extending).
11. Press `Enter` to save your changes.

    For more information about the Stations with Off-PBX Telephone Integration screen and field descriptions, see the *Avaya Aura® Communication Manager Screen Reference*.

    For more information on the **Location** field, see the *Avaya Aura® Communication Manager Screen Reference*.

    For more information about the off-pbx-telephone station-mapping commands, see the *Maintenance Commands for Avaya Aura® Communication Manager Branch Gateways and Servers*.

Setting up Feature Access Codes for Extension to Cellular

Procedure

1. Enter `change feature-access-codes`.
2. Type access codes according to your dial plan for the applicable features.

   Page down to access all pages of this screen.
3. Press `Enter` to save your changes.

A user can now activate Communication Manager features from any telephone through the FACs. A user can access the FACs through one of these three methods:

- Dialing the telecommuter number
- Dialing the remote access number
- Dialing the Select Idle FNE

After hearing the dial tone, the user enters the FAC.

Creating a telecommuting access number

Procedure

1. Enter `change telecommuting-access`.
2. In the **Telecommuting Access Extension** field, type an extension in accordance with your dial plan.

   The telecommuting number must be a direct inward dialing (DID) or central office (CO) trunk destination for off-premises features to work.
3. Press `Enter` to save your changes.
4. Provide your users with the telecommuting access number to enable or disable *Extension to Cellular*, or to change their Station Security Code.

Setting up Feature Name Extensions set

Procedure

1. Enter `change off-pbx-telephone feature-name-extensions set <n>`.
2. From your dial plan, enter the FNE numbers in the **Extension** field next to each feature.
3. Press `Enter` to save your changes.
4. Provide the FNEs to the user.

   Note:

   Administer up to 99 FNE sets on duplicated servers.

   Note:

   A pocket-sized FNE reference card is located on the last page of the *Avaya Extension to Cellular User's Guide*, 210-100-700.

A user can now access any of these Communication Manager features from their cell phone by dialing an FNE.

Creating a Self Administration Feature access code

Procedure

1. Administer the office extension to accept an Extension to Cellular telephone number.

2. Administer the SAFE Feature Access Code

   Note:

   The SAFE feature only works with EC500, PBFMC, SPFMC, and CSP. SAFE applies to any EC500, PBFMC, SPFMC, or CSP phone number administered. A system administrator must enter all other mapped phone numbers.

Administering the office extension for SAFE

About this task

You must set up the office telephone extension to accept an Extension to Cellular telephone number before the user can self administer their cell phone number using SAFE.

Procedure

1. Enter `add off-pbx-telephone station-mapping`.
2. For the office telephone extension, leave the **Phone Number** field blank.
3. Select **Enter** to save your changes.

   This procedure maps an office telephone extension to a blank cell phone.
4. Provide the SAFE access code to the user.

   The user calls the SAFE access code and enters their cell phone number.

   The cell phone number is now mapped to the office telephone. With SAFE, the user can also change their cell phone number.

   Immediately after the user enters a phone number, the system verifies that the phone number can be routed.

   - If the phone number is routable, the user hears confirmation tone.
   - If the phone number is not routable, the user hears intercept tone. The connection is not made.

Administering the Self Administration Feature Access Code

Procedure

1. Enter `change feature-access-codes`.
2. Page down to advance to the page containing the **EC500 Self Administration Access Codes** field.
3. In the **EC500 Self Administration Access Codes** field, type the access code according to your dial plan.

   You can administer up to four SAFE FACs for up to four applications, including EC500, PBFMC, CSP, and SPFMC supported on your system. The order of the SAFE FACs administered in this field applies to the order of the SAFE supported applications as they appear on the station mapping form.
4. Select `Enter` to save your changes.

The Extension to Cellular user can administer only one Extension to Cellular telephone number using SAFE. An administrator must map all other telephone numbers to the office telephone.

For more information about the Feature Access Code screen, see *Avaya Aura® Communication Manager Screen Reference*.

Creating FACs to enable/disable Extension to Cellular

Procedure

1. Enter `change feature-access-codes`.
2. Page down to advance to the page containing the **Enhanced EC500 Activation** field.
3. Type access codes according to your dial plan for the following fields.
   - **Enhanced EC500 Activation** field, used for remote activation of Extension to Cellular.
   - **Enhanced EC500 Deactivation** field, used for remote deactivation of Extension to Cellular.
4. Select **Enter** to save your changes.

   Users also have the option to activate and deactivate Extension to Cellular through a feature button on their office telephone. However, that feature button must be administered.

Creating a Station Security Code FAC

Procedure

1. Create a system-wide SSC change FAC.
2. Define the Station Security Code length.

Creating a system-wide SSC change FAC

Procedure

1. Enter `change feature-access-codes`.
2. Page down until the page displays the **Station Security Code Change Access Code** field.
3. Type a code valid for your dial plan in the **Station Security Code Change Access Code** field.

   This number is the FAC for this feature.
4. Select **Enter** to save your changes.

Defining the Station Security Code length

Procedure

1. Enter `change system-parameters security`.

2. Page down until the system displays the **Minimum Station Security Code Length** field.
3. Based on your dial plan, type a number in the **Minimum Station Security Code Length** field.

   This number determines the minimum required length of the SSC. Longer codes are more secure
4. Select **Enter** to save your changes.

   Users can now change their SSC only to a number with the specified number of digits.

   For more information about security, see *Administering Avaya Aura® Communication Manager*.

Administering an Extension to Cellular enable/disable feature button

Procedure

1. Change the EC500 state on the station form.
2. Administer the feature button.
3. Set the optional timer.

Note:

Feature buttons are only available on desk set telephone types that support administrable feature buttons.

Changing the EC500 state on the station form

Procedure

1. Type change station n where n is the extension of an Extension to Cellular station.
2. Go to page 2.

   Set the EC500 State as enabled or disabled.

Administering the enable/disable feature button

Procedure

1. Enter `change station n`, where *n* is the extension of an Extension to Cellular enabled station.
2. Page down until the **Button Assignments** field displays.
3. Select an available feature button under the Button Assignments header.

   Enter `ec500` to administer an Extension to Cellular feature button on the office telephone.
4. Select **Enter** to save your changes.

   The user of the station can now use that feature button to enable and disable Extension to Cellular.

Note:

The **Timer** subfield is displayed next to the ec500 Button Assignment, and defaults to n. Leaving the default setting of n excludes the timer state.

Setting the disable Extension to Cellular timer

About this task

Users can also use a timer to temporarily disable Extension to Cellular.

Procedure

1. In the Station screen, locate the **Timer** subfield next to the ec500 **Button Assignment**.
2. Set the **Timer** subfield to `y` to enable an Extension to Cellular timer state for the administered feature button.
3. Select **Enter** to save your changes.

   The corresponding feature button on the office telephone is now administered for Extension to Cellular. The user can activate a one-hour timer to temporarily disable Extension to Cellular through this administered feature button.

Administering the extnd-call feature button through SAT

Procedure

1. Type `change station n`, where *n* is the extension of an Extension to Cellular-enabled station.
2. Page down until you see the **Button Assignments** field.
3. Select an available feature button under the **Button Assignments** field.
4. Type `extnd-call`.
5. Select **Enter** to save your changes.

   The corresponding feature button on the office telephone is now administered to extend calls between the office telephone and the Extension to Cellular cell phone.

Administering the extnd-call feature button through System Manager

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, do one of the following:
   - To create a CM Endpoint profile for a new user profile, click **New**.
   - To create a CM Endpoint profile for an existing user, select the user and click **Edit**.
3. Click the **Communication Profile** tab.

4. In the PROFILES section, click the toggle button next to **CM Endpoint Profile**.

   System Manager enables **CM Endpoint Profile** and displays the fields of the CM Endpoint profile.
5. Click **Endpoint Editor**.
6. On the Edit Endpoint page, click the **Button Assignment** tab.
7. On the **Main Buttons** tab, select `extnd-call` from the drop-down list box.
8. Click **Done**.

Reviewing Extension to Cellular feature button assignments

Procedure

1. Enter `change display-messages view-buttons`.
2. Page down to view subsequent screens.

   If you assigned feature buttons to enable/disable Extension to Cellular and to extend a call between the office and cell phone, you can see **EC500** and **Extend Call** in the feature button list.

   Note:

   The **EC500** button refers to the Extension to Cellular enable/disable feature button.
3. Select **Enter** to save your changes.

Viewing the button labels for the feature buttons

Procedure

1. Enter `change display-messages button-labels`.
2. Page down to view all screens. If administered, you see the EC500 and Extend Call labels.
3. Select **Enter** to save your changes.

Sending 10-digit caller identification for locally originated calls

About this task

The following procedure is for cell phone use only.

Procedure

1. Enter `change public-unknown-numbering`.
2. **Under the Ext Len** field, type an extension length between 0 and 7.
3. **Under the Ext Code** field, type the starting digit(s) of the extension, such as the country code.
4. **Leave the Trk Grp(s)** field blank to apply to all trunks in the system.

5. Under the **CPN Len** field, type `10` to indicate a 10-digit calling number.
6. Press `Enter` to save your changes.

   This administration adds a prefix to extensions to create a 10-digit calling number for locally sourced calls.

Administering Confirmed Answer for Cellular Voice Mail Avoidance

Procedure

1. Enter `change off-pbx-telephone configuration-set n`, where *n* is the number assigned to the **Configuration Set** field of the user's off-pbx-telephone station-mapping screen.
2. In the **Confirmed Answer** field, type `y`.

   The system displays the **Timeout** field with a default value of 10. The values are 5 to 20 (seconds).
3. Select **Enter** to save your changes and exit the system.

Administering call filtering for Extension to Cellular

Procedure

1. Enter `add off-pbx-telephone station-mapping`.
2. Proceed to page 2 of the Stations with Off-PBX Telephone Integration screen.

   The second page displays the information that you have entered in the **Station Extension** field on the first page as read only information.
3. Enter the acceptable type of call under the **Calls Allowed** field for each Station Extension.

   Calls allowed can be internal, external, all, or none.
4. Select **Enter** to save your changes.

   For more information on the **Calls Allowed** field, see *Avaya Aura® Communication Manager Screen Reference*.

Administering voice mail coverage for Extension to Cellular

Procedure

1. Set up a Cellular Voice Mail Avoidance timer.
2. Use timing to route calls to voice mail.

Setting up a Cellular Voice Mail Avoidance timer

Procedure

1. Enter `change off-pbx-telephone configuration-set n`, where *n* is the number assigned with a coverage path.
2. In the **Cellular Voice Mail Detection** field, type `timed`.

   The system displays the **(seconds)** field, with the default value of 4. The values are 1 to 9.

   Note:

   The default value for this field changed from none to timed starting in Communication Manager Release 5.0. However, if the system is upgraded from older releases, the default setting will remain as none.
3. If you want to increase the time before the cell phone routes to coverage, change the **(seconds)** field.

   For example, set the timer to 5 seconds.
4. Select **Enter** to save your changes.

   For more information about the Configuration Set screen, see *Avaya Aura® Communication Manager Screen Reference*.

Using timing to route calls to voice mail for Extension to Cellular

Procedure

1. Enter `change coverage path n`, where *n* is the number assigned with a coverage path.
2. Change the value in the **Number of Rings** field as appropriate.

   The number of rings must be less than the number of unanswered rings before the cellular service provider voice mail covers a call.
3. Select **Enter** to save your changes.
4. Remind users that they must disable Extension to Cellular before turning off their cell phone.

   This action prevents messages from automatically going to cellular voice mail and ensures that corporate voice mail covers all business calls.
5. Remind users with business-only cell phones that they can ask their cellular provider to turn off cellular voice mail.

Setting up Call Detail Recording for Extension to Cellular

Procedure

1. Enable CDR for the outgoing trunk.
2. Enable CDR for Extension to Cellular.

3. Generate CDR records.

Enabling CDR for the outgoing trunk for Extension to Cellular

Procedure

1. Enter `add trunk-group n`, where *n* is a new trunk group number.
2. Type `y` in the **CDR Reports** field to enable CDR.
   - Type `y` to track calls to cell phones for reporting or charging purposes.

     If you type `y`, the configuration set administered on the Station screen determines whether a CDR record is generated.
   - Type `n` if you want to treat the Extension to Cellular cell phones as totally internal stations and do not require CDR reporting.
3. Select **Enter** to save your changes.

Enabling CDR for Extension to Cellular

Procedure

1. Enter `change off-pbx-telephone configuration-set n`, where *n* is the number assigned with a coverage path.
2. In the **CDR for Calls to EC500 Destination** field, type `y` to enable CDR.
3. Select **Enter** to save your changes.

   When this field is set to y, an outgoing trunk CDR report is created for each Extension to Cellular call.

Related links

Call Detail Recording administration on page 455

Generating CDR records with Extension to Cellular

Procedure

1. Enter `change system-parameters cdr`.
2. Set the **Intra-Switch CDR** field to `y`.
3. Select **Enter** to save your changes.
4. Log off and log back into the switch.
5. Enter `change intra-switch-cdr`.
6. Type any extension you want to track with this screen.
7. Select **Enter** to save your changes.

Note:

There is no intra-switch-cdr record when using originating CDR.

Changing configuration sets for Extension to Cellular

Procedure

1. Enter `change off-pbx-telephone configuration-set n`, where *n* is the number that you assign to a configuration set.
2. In the **Configuration Set Description** field, type in a description of the configuration set, up to 20 characters.
3. Type the Calling Number style as either network or pbx.

   The **Calling Number Style** field determines the caller ID format for calls from a local switch extension to an Extension to Cellular cell phone.
4. Type an entry in the **CDR for Origination** field to determine the CDR report format that Communication Manager will use for the originator of an incoming call.

   The CDR report provides the calling party number of the incoming calls. If you select the extension option, the internal Extended Access extension is reported as the calling party. If you select the phone number option, the reports displays the 10-digit cell phone as the calling party number. If you use the none option, there will be no originating CDR record.
5. Enter `y` or `n` for the **Fast Connect on Origination** field to determine whether additional processing occurs on the switch before connecting a call.

   You can use this option to check the capabilities provided by the cell phone provider. Currently, Avaya recommends the default value of n. The downside of Fast Connect is that there is no indication to the caller of when the far-end has actually answered. The billing of the call starts immediately after the call setup. If billing is involved, then do not select the **Fast Connect** option. However, all digits required to route the call must be passed in the SETUP message. DECT XMOBILE stations always use Fast Connect. Whereas, PHS XMOBILE and EC500 XMOBILE/OPTIM stations never use Fast Connect. SIP phones do not block blind conference if the **Fast Connect** option is enabled.
6. Verify that the default dtmf is the entry for the **Post Connect Dialing Options** field.

   The **Post Connect Dialing Options** field determines whether additional capabilities are available for incoming ISDN trunk calls that are mapped into Extension to Cellular stations. These capabilities are beyond standard ISDN dialing.
7. Verify that the **Calling Number Verification** field is set to the default value y.

   Important:

   The default value y restricts incoming calls to “network provided” or “user provided verified and passed” calling numbers. When the switch is part of a private network and you are not screening calling numbers, change the field to n.
8. In the **Confirmed Answer** field, enter `y` or `n`.

   If y, set the timeout period for waiting for user input of a digit. When set to y, a digit must be received within the time out period, or the call is not treated as answered. The default time out period is 10 seconds.

9. In the **Call Appearance Selection for Origination** field, enter `primary-first` if you want to select regular call appearance first for origination or enter `first-available` if you don't care whether a regular or bridged appearance is selected for origination.
10. In the **Use Shared Voice Connections** field, enter `y` if you want to share a single trunk for a cell phone call and a PBX call.

    You can use shared voice connection option only with the FMC applications such as PBFMC, PVFMC, and SPFMC.
11. In the **Apply Ringback Upon Receipt of** field, enter `Call-Proceeding` to configure Communication Manager to send the ringback tone to the caller immediately or enter `Alert` to configure Communication Manager to wait for the ALERT message from the network before sending the ringback tone to the caller.
12. Select **Enter** to save your changes.
13. Use the **`change off-pbx-telephone configuration-set`** *n* command as needed to change additional configuration sets.

Related links

Call Detail Recording administration on page 455

Administering the barge-in tone for Extension to Cellular

Before you begin

Before the barge-in tone can be used, a Intrusion tone must be set up on the Tone Generation Customized Tones screen. To verify that a Conference tone is set up, type `change tone-generation` *n*, where *n* is a number between 1 and 50.

Important:

The barge-in tone is a type of intrusion tone. You may have to set up an intrusion tone if the default is silence. If default intrusion tone is not set to silence (as in the United States), you do not have to administer it, but you can change the characteristics of the tone.

About this task

Procedure

1. Enter `change off-pbx-telephone configuration-set` *n*, where *n* is the number assigned with a coverage path.
2. In the **Barge-in Tone** field, select y to enable or n to disable.
3. Press `Enter` to save your changes.

   When the barge-in tone is enabled, all parties on a call hear a conference tone if all of the following conditions are true:

   - The conference tone is administered in the country form
   - Extension to Cellular is enabled
   - The exclusion feature is disabled

- A user is on the conference call on their cell phone
- Another user tries to join this call on the Extension to Cellular-associated office telephone

Displaying System Capacity for Extension to Cellular

Procedure

1. Enter `display capacity`.
2. Page down to the **Off-PBX Telephone - PBFMC**, **Off-PBX Telephone - PVFMC** fields.
3. View the capacities and press **Next**.
4. View the memory capacities and press **Cancel** to exit the screen.

Administering Conditional Call Extending for Extension to Cellular

Procedure

1. Enter `change off-pbx-telephone station-mapping`.
2. Fill in the information in all fields for each Station Extension.
3. Proceed to page 3 of the Stations with Off-PBX Telephone Integration screen.

   The third page displays the information that you have entered in the **Station Extension** and **Application** fields on the first page as read only information.
4. Type `y` for the required call type in the **Calls Accepted** field.

   Type `n` for the call type that you want to restrict. The call types that you can allow or restrict are:

S	Standard calls to the station
C	Calls covered or forwarded to the station
H	Calls to the station through a hunt group
I	Intercom calls to the station
P	Priority calls to the station
R	Calls restricted by a COR permission matrix

5. Type the class of restriction number in the **COR** field.
6. Select **Enter** to save your changes.

Administering Sharing Mapping among Communication Manager PBXs for Extension to Cellular

About this task

With the Sharing Mapping among Communication Manager PBXs feature, you can share station name and station mapping information with multiple Communication Manager servers. A Communication Manager server acquires mapping information from other Communication Manager servers by using a SIP subscription. Communication Manager subscribes for the shared mapping on the Off-Pbx-Telephone Mapping-Subscriptions screen. SIP trunks or Subscription Aggregator is used to interconnect Communication Manager servers to share mapping information. Each Communication Manager server can make up to 3 subscriptions.

Procedure

1. Type `change off-pbx-telephone mapping-subscriptions`. Press `Enter`.

   The system displays the Mapping Subscription screen.

2. In the **Signaling Group** field, specify the signaling groups for a far-end domain of PBX or subscription aggregator.
3. In the **Level** field, specify the subscription level for a far-end PBX or subscription aggregator.
4. In the **Maximum Percentage of Mapping Storage Allowed for Acquired Mappings** field, specify the maximum percentage of mapping storage that is allowed for the acquired mappings.

   Note:

   Mapping storage is shared between Administered Mappings, Acquired Mappings, and ONE-X Mappings.

   You can use the `list mappings-acquired` command to list acquired mappings.

5. Using the `off-pbx-telephone station-mapping` command, go to page 3 of the Stations With Off-PBX Telephone Integration screen. Compare the subscription level with the share level. If the share level is less than the subscription level, the system discards the mapping.

   The information on this page maps to the information that you have entered in the **Station Extension** and the **Application** fields on the first page.

Administration for Avaya one-X Client Enablement Services

Procedure

1. Enter `change cor n`, then go to page 3 of the screen.
2. Set the one-X Server Access to y to allow one-X control.
3. You can list the stations currently under one-X control using the **`list off-pbx-telephone station-mappings`** command.

4. You can see the one-X status of the stations that are controlled using **`status station`** command.

   Field **one-X Status** values are: blank, normal, no-ring, trigger, coverage, voice mail, or N/A. If the value is normal, then the station's behavior is unaffected by the one-X Server. When the value is no-ring, then the station will not ring under any conditions. If the value is triggered, the decision to ring the station is controlled by the one-X Server on a call by call basis. If the value is coverage or voice mail calls to the station will immediately cover, if possible.

Setting up One-X Server integration

Procedure

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

End-user procedures for Extension to Cellular

End-users can activate or deactivate certain system features and capabilities. End-users can also modify or customize some aspects of the administration of certain features and capabilities. For more information on end-user procedures, see the *Avaya Extension to Cellular User's Guide*, 210-100-700.

Extension to Cellular upgrades from prior versions

Extension to Cellular is available only with Communication Manager Release 1.3 or later. The Extension to Cellular releases can be administered and operated concurrently on the same Avaya server running Communication Manager. You can continue to support users with Extension to Cellular releases 1 through 4.1. Or you can upgrade all users to the latest version of Communication Manager.

Note:

Endpoints configured as XMOBILE cannot access important enhancements to EC500, such as support for SIP trunk groups. You must follow the steps in this section to gain access to these enhancements for your EC500 users.

If you are converting from Extension to Cellular versions 1-4 you must perform the following steps to update to the latest version as part of Communication Manager Release 5.2 or later:

1. Enter `change station n`, where *n* is the station you want to change.

2. Set the XMOBILE Mapping Mode to `none`.

   All previous mapping of XMOBILE stations, the way Extension to Cellular used to be administered, cannot interfere with *Extension to Cellular*.

3. Set up the new office telephone to cell phone mapping in Mapping an office telephone to a cell phone.
4. Test the system.
5. If the system works, remove the XMOBILE station records.

   This last step frees up stations that go toward the maximum number of stations allowed.

Starting with Extension to Cellular 5.0 (Communication Manager Release 2.0) introduced support for the Off-PBX Telephone Integration and Mobility (OPTIM). Once XMOBILE Mappings are converted to OPTIM, further upgrades from that release to higher releases are automatic. Only new capabilities need to be administered when upgrading to new releases. Some of those include:

- Support of up to 4 OPTIM applications per station extension – up to 4 phone number mappings can be administered per station extension.
- Self Administration Feature (SAFE) Access Codes so users can enter and change their own cell phone numbers. For more information, see Creating a Self Administration Feature (SAFE) access code. Using this feature, you can have up to 4 SAFE Access Codes per extension to modify up to four phone numbers per extension.
- Administration of the barge-in tone for added security. For more information, see Administering the barge-in tone.
- Mapping dialed extensions to the new Feature Name Extensions. For more information, see Setting up Feature Name Extensions (FNE)s.
- Support of multiple sets of Feature Name Extensions.
- Fixed Mobile Convergence (FMC) applications support PBFMC and SPFMC. PVFMC applications support dual-mode cellular phones.

See Detailed description of Extension to Cellular for a list of all OPTIM capabilities.

Upgrades from *Extension to Cellular* Version 5

The following administration tasks are new in Extension to Cellular Version 6:

- Setting up the Self Administration Feature (SAFE) Access Code so users can enter and change their own cell phone number. For more information, see Creating a Self Administration Feature access code.
- Administering the barge-in tone for added security. For more information, see Administering the barge-in tone.
- Mapping dialed extensions to the new Feature Name Extensions. For more information, see Setting up Feature Name Extensions set.

Upgrading from *Extension to Cellular* Version 4

About this task

To administer an *Extension to Cellular* feature button and include the optional *Extension to Cellular* timer:

Procedure

1. Enter `change station n`, where *n* is the extension of an *Extension to Cellular*-enabled station.
2. Press the **Next Page** button twice to display page 3 of the Station screen.
3. Select an available feature button under **BUTTON ASSIGNMENTS** and type `EC500`. Press `Enter`.

   The system displays the **Timer** subfield, which defaults to n. Leaving the default setting of n excludes the timer state.
4. 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*.

   The corresponding feature button on the office telephone is now administered for *Extension to Cellular*, and configured with the optional *Extension to Cellular* timer.

   Note:

   The feature status button on the office telephone indicates the current state of *Extension to Cellular*. The status is displayed regardless of whether the feature was enabled remotely or directly from the office telephone.

Upgrading from *Extension to Cellular* Version 3

About this task

The following process is to change the *Extension to Cellular* configuration to work without the loopback trunks. Let us eliminate the loopback connections for station 5462.

Eliminating the loopback trunks is optional and must be accompanied by changing the **Mobility Trunk Group** field on the Station screen to ars.

Procedure

1. Eliminate the DS1 or IP loopback trunks associated with *Extension to Cellular* Version 2.0 or 3.0.

   This step includes removing the loopback trunks and signaling groups through switch administration and physically from the switch.

   Loopback trunk configuration can coexist with the *Extension to Cellular* R4 if you choose to do so. If you decide to eliminate the loopback trunks, the removed equipment can be reused for other trunk solutions. You can change gradually over to a total loopback

elimination. If you decide to have the loopback and non loopback configurations coexist, you must remember there are capacity restrictions when using the DS1.

2. Enter `change station n`, where *n* is the extension of an Extension to Cellular-enabled station.
3. In the **Mobility Trunk Group** field, type `ars`.

   The field must be changed to ars for loopback elimination.
4. Press `Enter` to save your changes.

   If the **Dial Prefix** field contains the ars Feature Access Code, remove the prefix.

   For more information, see the *Administering Avaya Aura® Communication Manager,*.

Upgrading from *Extension to Cellular* Version 2

About this task

Implement changes as described for upgrade from *Extension to Cellular* Version 3.

Starting with Version 3, there is a field on the Station screen called Mapping Mode. There is a command, **`list xmobile mapping`**, that makes it easy to find out the XMOBILE extensions and primary extension associated with a cell phone number. The **`status station`** command now explicitly shows the *Extension to Cellular* state: enabled or disabled.

Procedure

1. Identify the station bridged to the second call appearance of the primary extension.

   The **`list bridged-extensions <primary ext>`** command provides this information.
2. Enter `change station <xmobile ext>`.
3. Change the **Mapping Mode** field to both.
4. Press `Enter` to save your changes.

   Note:

   If the **Cell Phone Number** field contains a dial prefix such as 1 for long distance, re-administer the cell phone number and place the prefix number in the **Dial Prefix** field. Also make sure that the full number, including area code, is in the **Cell Phone Number** field. This number is necessary for office caller ID to function.

   For information on installation and administration of Version 2 of *Extension to Cellular*, see *Avaya EC500 Extension to Cellular Installation and Administration Guide*, Issue 2, July, 2001.

Upgrading from Version 1

About this task

For pre-existing stations, you can continue to use ARS digit conversion to convert the extension to a cell number or they can be changed to use the new fields on the Station screen.

Procedure

1. Enter `change station` *`xmobile ext`*.
2. Type each dial prefix, if any in the **Dial Prefix** field. For example, type `1` for long distance, but not 9 for external access.
3. Type the full cell phone number including area code in the **Cell Phone Number** field.
4. Type `termination` in the **Mapping Mode** field.
5. Select **Enter** to save your changes.

   For information on installation and administration of Version 1 of *Extension to Cellular*, see *Avaya EC500 Extension to Cellular Installation and Administration Guide*, Issue 1, February 8, 2001.

Interactions for Extension to Cellular

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

Attendant

If the **Calls Allowed** field on the Stations with Off-PBX Telephone Integration screen is internal, attendant-originated and attendant-extended calls are not delivered.

Call coverage

Manipulate the number of unanswered rings on the cell phone If you want to ensure that unanswered calls go to office voice mail instead of the cell phone's voice mail. Set the value in the **Number of Rings** field on the Coverage Path screen for the office telephone to a lower number than the voice mail coverage setting on the corresponding cell phone. For more information, see Administering voice mail coverage.

Call Detail Recording

A Call Detail Recording (CDR) record is generated for calls that originate from an Extension to Cellular cell phone. For this feature to work, incoming trunk CDR must be turned on. The system does not generate a CDR if the user dials a Feature Name Extension (FNE) that does not result in a call.

Cellular service provider voice mail

Office stations can have standard Avaya server running Communication Manager voice mail coverage such as Communication Manager Messaging. But cell phones usually have voice mail coverage from the cellular service provider. There are now two ways to coordinate the two systems.

First, you can administer Communication Manager Extended Access Cellular Voice Mail Avoidance. Use the Cellular Voice Mail Avoidance feature to reduce the uncertainty as to

where unanswered Extension to Cellular calls go. An unanswered call ends either at your office telephone voice mail, or at your cell phone voice mail system.

Communication Manager detects when the cell phone is not the entity that answers the call and brings the call back to the server. The call is treated as a normal call on the telephone with Extension to Cellular enabled. The call is then processed with the normal number of rings set on your call coverage.

Second, you can set up the number of unanswered rings so that one of the voice mail systems always answers first. However, there are coverage options in both the Avaya server running Communication Manager and the network that send a call immediately to the respective voice mail. Examples of these options include “busy,” “active,” or “send-all-calls” in Communication Manager and “cell phone unavailable” or “network congested” in the network. Users must understand that an unanswered call can result in a voice mail message in either mailbox.

Class of Restriction

For calls toward an *Extension to Cellular* station, Class of Restrictions are applied normally for a call terminating to a station. In particular, if the station is mapped, then the Class of Restriction (COR) of the office telephone applies. Any restrictions imposed by call filtering are applied after those imposed by the COR. Calling party restrictions pertaining to trunks do not initiate *Extension to Cellular* calls. These restrictions include “outward,” “tac-toll,” and “all-toll.”

Its important to note that a phone may be restricted from making outside calls but the Extension to Cellular calls can be extended to the cell phone.

Distributed Communications System

Interswitch calls on Distributed Communications System (DCS) trunks are treated as internal calls.

- When an *Extension to Cellular* user has the **Calls Allowed** field on the Stations with Off-PBX Telephone Integration screen set to internal or all, DCS calls are delivered to the cell phone.
- When an *Extension to Cellular* user has the **Calls Allowed** field set to external or none, DCS calls are not delivered.

Distinctive alerting

Cell phones might not receive distinct rings for different types of calls. Check with your cellular service provider.

Extension to Cellular enable and disable

Extension to Cellular can be enabled or disabled. Users can enable or disable Extension to Cellular calls with either FACs or the enable and disable feature status button.

Users who receive their Extension to Cellular service through their cellular service provider (CSP) cannot enable or disable their Extension to Cellular calls. Through CSP, Extension to Cellular is always enabled.

Feature Access Codes

A user can activate Communication Manager features through Feature Access Codes (FACs). For more information on setting up feature access codes, see Setting up Feature Access Codes for Extension to Cellular on page 775.

Feature Name Extensions

When *Extension to Cellular* is enabled, a user can activate a Communication Manager feature through dialing a Feature Name Extension (FNE) from the cell phone or SIP endpoint. Feature

name extensions correspond to a direct inward dialing (DID) number for each feature. Each FNE must match your dial plan, and are administered system-wide.

Message waiting indication

Cell phones cannot receive a screen that indicates a message waiting directly from Communication Manager.

“Notify me” under Unified Messenger for MS Exchange

The “notify me” feature of Unified Messenger® for Microsoft Exchange® (Version 4.0 or later) notifies users of messages in the corporate voice mailbox through the cell phone display. For more information on using this feature, see “Setting Notify Me” in the *Unified Messenger Telephone User Interface Online Guide*, accessed through http://www.avaya.com/support.

Note:

The cell phone must support text messaging to use this feature.

Office caller ID for another user

Incoming calls from other *Extension to Cellular* users are internal calls if office caller ID is enabled for the station associated with the cell phone.

- When an *Extension to Cellular* user has the **Calls Allowed** field set to internal or all, the *Extension to Cellular* calls are delivered.
- When an *Extension to Cellular* user has the **Calls Allowed** field set to external or none, calls from other *Extension to Cellular* users are not delivered.

QSIG

Inter-PBX calls on QSIG trunks are treated as internal calls.

- When an *Extension to Cellular* user has the **Calls Allowed** field set to internal or all, QSIG calls are delivered.
- When an *Extension to Cellular* user has the **Calls Allowed** field set to external or none, QSIG calls are not delivered.

Service Observing

You cannot activate the Service Observe feature from numbers mapped with EC500. If a call comes in from a number mapped with EC500, Communication Manager considers the call to be bridged appearance. If you use bridged call appearance, you cannot use Service Observing.

Extension to Cellular troubleshooting

This section lists the known or common problems that users might have with the Extension to Cellular feature.

Extension to Cellular installation and administration test

After you have administered Extension to Cellular, use the following installation test procedures to ensure that the Extension to Cellular solution performs as expected. These tests are for Extension to Cellular cell phone use only.

The Extension to Cellular installation test and customer acceptance procedures follow the same guidelines used for testing a new station added to the switch. However, a review of the basic test procedures is provided in this section.

Testing Extension to Cellular functionality and voice mail coverage

About this task

When performing this test, you might need to place several calls to the Extension to Cellular cell phone.

Procedure

1. Dial the office telephone number with any other touchtone telephone.
2. Ensure that the office number and the Extension to Cellular cell phone ring simultaneously.
3. When the cell phone rings, verify that a ten digit ANI is displayed on the cell phone.
4. Verify that the call covers to the primary voice mail account (which is usually the corporate office voice mail box).

   If the call does not cover properly, review the coverage path number of rings and setup for corporate voice mail coverage.

   To get the voice mail coverage that you want, you can experiment with the number of rings set for the cellular service provider and for the office number coverage path. For more information about sending office caller ID, voice mail administration, and call forwarding, see the Detailed description of Extension to Cellular.

Testing the second call appearance for Extension to Cellular

Procedure

1. Dial the office telephone number with a touch-tone telephone.
2. Answer the call that is ringing on the cell phone to start your test conversation.
3. With the test conversation in place and active, place another call to the office telephone number using any other touchtone telephone.

   The call must ring at the second call appearance on the office telephone, and at the cell phone. The display screen on the cell phone must show the second incoming call.
4. Answer the second call with the call waiting feature on the cell phone.

   If any of the test procedures fail, you must verify that all administration entries were input correctly.

Extension to Cellular trouble resolutions

Problem	Possible Cause	Action
Users cannot receive Extension to Cellular calls on their cell phones.	For more information on possible sources of the problem, see Call Distribution methods for hunt group types on page 840.	For detailed instructions on troubleshooting this problem, see Call Distribution methods for hunt group types on page 840.
No CDR for Extension to Cellular calls.	The Configuration Set for the Extension to Cellular station has the **CDR for Calls to EC500 Destination** field set to n. The Extension to Cellular station is still using loopback trunks. The CDR Reports option on the trunk being used is n.	Check administration of Configuration Set screen, the Stations with Off-PBX Telephone Integration screen, or the Trunk Group screen, and change if necessary.
	Neither the principal station or other station extension is administered in the intra-switch-cdr screen.	Add one or both extensions in the intra-switch-cdr screen.
Call drops when user answers a cell phone.	Cellular Voice Mail Avoidance timeout is too long.	Shorten timeout. Train user to wait before answering cell phone. Remove user from Cellular Voice Mail Avoidance.
FNEs not working.	• Misadministration. • Calling Number Verification set to y on Configuration Set screen.	• Verify that the telephone number on off-pbx station-mapping screen is a full national number (10-digits in America and UK) and does not contain any a prefix digits like country code • For security, the option should be set to y. However, if calls always come over private trunks, you can set the option to n.
The user cannot access Feature Name Extensions by dialing the corresponding FNE.	There is no corresponding number administered on the Off-Pbx-Telephone Feature-Name-Extension screen or the mapping mode is not origination or both.	Administer an extension on the off-pbx-telephone feature-name-extension screen, or change the mapping mode to origination, or both. Change the Cellular Voice Mail Detection option to timeout. This will handle any cell network condition (congestion, cell phone off, and so on) that causes the

Table continues…

Problem	Possible Cause	Action
User reports many unanswered calls are going to cellular voice mail.	Cellular Voice Mail Detection option (in user's configuration set) is not appropriate for cellular service provider. The no answer timeout for cellular voice mail is too short	call to go immediately to cellular voice mail. Have user contact service provider to lengthen the no answer timeout so that it is longer than the coverage path timeout. This will ensure that unanswered calls ringing at the cell phone will go to the corporate voice mail. Discuss with user using the confirmed answer option. This option handles a common occurrence not handled above. A cell phone out of network coverage will go to cellular voice mail after about 3 rings. This is too long for Cellular Voice Mail Detection and too short for a coverage path fix.
User reports desk set does not ring, rings only once, or that callers are sent immediately to cellular voice mail.	Cell phone is off and calls are immediately being sent to cellular voice mail.	Change the Cellular Voice Mail Detection option to timeout (in user's configuration set).
The user reports that the cell phone is not receiving caller identification numbers for calls from the Avaya server running Communication Manager. But, the office number that the cell phone is mapped to does.	The Avaya server running Communication Manager has not been administered properly for sending caller identification numbers. Most cellular service providers require a number in national format.	Recheck the outbound trunk screen to ensure that the **Send Calling** field is set to y.
	External trunks serving the cell phone are using a non-ISDN trunk.	Change the routing administration to route over an ISDN trunk.
The user reports that the person being calling is receiving the incorrect caller ID.	The Configuration Set screen has the **Calling Number Style** field set to PBX.	Change the **Calling Number Style** field on the Configuration Set screen to network.
	There is an incorrect entry on the ISDN public-unknown numbering screen.	Verify that the entries on the ISDN public-unknown numbering screen are correct.

Table continues…

Problem	Possible Cause	Action
The user reports that the cell phone is receiving a switch default caller identification number for calls from the Avaya server running Communication Manager.	The ISDN Service Provider (SP) is replacing the caller identification with a fixed caller ID.	This is generally not solvable within the PBX. Escalate the issue to your Telecom Manager. The manager can contact your ISDN SP to request a solution or an alternate ISDN SP that allows the caller identification to pass. Some service providers will pass the caller ID if special application SA8931 is enabled. This sends the user's station (DID) number as a redirecting number in addition to the original calling number. In some instances special application SA8983 is helpful. When this option is on, the user's station (DID) number is sent as the calling number to the cell phone. This distinguishes EC500 calls from direct calls to the cell phone.
	The switch is blocking the outgoing caller identification and is passing a default caller ID.	Change your switch administration to allow caller identification to go outside the switch.
The user hears a beep while on a call originating from the Avaya server running Communication Manager. The user cannot use the call waiting feature on the cell phone to switch to the other call.	Most likely the user is hearing the tone provided by the Avaya server running Communication Manager when call waiting is enabled at the switch.	You have two possibilities: 1) Communicate to the user that when a call waiting indication is heard, but the user cannot switch the call, the user must disconnect on the first call to receive the second call, OR 2) Disable call waiting at the switch level. The regular call waiting capability provided by the cellular service provider then handles the call waiting feature.

Table continues…

Problem	Possible Cause	Action
The Extension to Cellular cell phone call into the office switch fails to provide the office caller ID.	The **Cell Phone Number** field administered for the Extension to Cellular station does not have the required entry, which almost always is the full national number.	Type the full caller ID number in the **Cell Phone Number** field. Remove any dialing prefixes such as long distance access code (1 in US and Canada, 0 in Europe and many other countries), international access code (011 in US and Canada, 00 in Europe and many other countries), or country code. The dialing prefixes should be administered in the **dial prefix** field, and country code in the **country code** field.
	Calling Number Verification set to y on Configuration Set screen.	Set Calling Number Verification to n. See FNEs not working.
	The **Mapping Mode** field administered for the Extension to Cellular station does not contain origination or both.	Type `origination` or `both` in the **Mapping Mode** field.
	The external inbound call is not entering into the switch over an ISDN trunk.	Contact the ISDN Service Provider to ensure that inbound calls come into the switch through an ISDN trunk.
	The external inbound call does not come into the switch on which the Extension to Cellular cell phone station is administered.	Create a station for the Extension to Cellular cell phone with the proper mapping on the switch that the call enters.
	The calling number is manipulated on the Inbound Trunk screen.	Administer the Extension to Cellular station **Cell Phone Number** field to match the modified calling number.
	The cellular service provider does not send the calling number.	Call the cellular service provider and request to activate sending of caller ID.
	Someone else was on a call simultaneously on the office telephone and on the same line appearance as the originating Extension to Cellular cell phone call.	Move the mapped line appearance to a button that is not likely used by another telephone call.

Table continues…

Problem	Possible Cause	Action
With the Avaya server running Communication Manager, you cannot have a default entry of extensions. For example, you cannot enter the # key alone to replace entering the extension followed by the # key.	The cell phone number is improperly mapped.	See The Extension to Cellular cell phone call into the office switch fails to provide the office caller ID. in this table.
An intercept tone is received when attempting to enable/disable Extension to Cellular For example, the tone chimes when you type the Feature Access Code, #, Station Security Code, and #.	The user has used the Station Security Code of the Extension to Cellular extension and the code is different from that of the principal.	The user must type the code of the principal extension.
	The Station Security Code is blank for the principal.	The Station Security Code for the principal must be administered.
When attempting to enable/disable Extension to Cellular, the user receives an intercept tone.	The **Applications** field administered on the Stations with Off-PBX Telephone Integration screen for the Extension to Cellular station is not EC500 or PBFMC.	Change the **Applications Extension** field on the Stations with Off-PBX Telephone Integration screen for the Extension to Cellular station to EC500 or PBFMC.
	The **Applications** field administered on the Stations with Off-PBX Telephone Integration screen for the Extension to Cellular station is EC500. But, the Configuration Set is not administered for DTMF.	Access the associated Configuration Set screen and ensure that the entry in the **Post Connect Dialing Option** field is DTMF.
The office caller ID is that of the origination mapped *Extension to Cellular* station and not of the host extension.	The *Extension to Cellular* station is not mapped to the host telephone.	Map the *Extension to Cellular* station to the host extension.
The administered Extension to Cellular feature button on the office telephone flashed for 2 seconds at the broken flutter rate.	The Extension to Cellular administration somehow got corrupted.	Disable, then enable, Extension to Cellular.
User cannot engage the Extension to Cellular timer through the administered feature button on the office telephone.	The optional Extension to Cellular timer is not configured.	Configure the optional Extension to Cellular timer on the Station screen.

Table continues…

Problem	Possible Cause	Action
The user receives the error Contact System Administrator when trying to enable/disable Extension to Cellular through the administered feature button on the office telephone.	The Stations with Off-PBX Telephone Integration screen is incorrectly administered.	Verify that all required information, in the correct format, is included on the Stations with Off-PBX Telephone Integration screen. In particular check that the **Dial Prefix**, **Country Code**, and **Phone Number** fields are administered correctly.
An Extension to Cellular station is mapped to a principal station, and the principal station later adds a configured Extension to Cellular feature access button. The **`status station`** command for the principal station shows that Extension to Cellular is disabled. The **`status station`** command for the mapped Extension to Cellular station shows that Extension to Cellular is enabled.	A previously administered and enabled Extension to Cellular station was mapped to a principal station that does not have an Extension to Cellular feature access button configured.	Configure an Extension to Cellular feature access button on the principal station. The principal station must support configurable feature buttons. See Administering an enable/disable feature button on page 779. When configured, press the Extension to Cellular feature access button to enable Extension to Cellular. This action synchronizes the enable/disable state between the principal station and its mapped Extension to Cellular station.
User reports cannot use Idle Appearance Select FNE to call certain extensions or external destinations.	The user is misdialing. The PBX has multiple locations, and an incorrect location is used for interpreting the dialed digits.	Administer the **location** field on the Stations with Off-PBX Telephone Integration screen with the location of the user's desk set. Since this field is not administrable for the EC500 application, it may need to be changed to PBFMC.
User hears dial-tone when answered an EC500 call.	User has the Confirmed Answer feature enabled on the configuration set form.	Instruct user to dial a digit after the dial tone.
User enters a digit after hearing dial tone, but is not cut through to the caller.	User is entering the digit too quickly.	Some cellular providers need almost a second to cut through a voice path after answer. Instruct user to pause between answering the phone and pressing the digit.
User dials the Self Administration for EC500 FAC and receives intercept tone.	The user is misdialing extension or security code. The user is not entering a number that is routable through ARS.	Instruct user in proper sequence for entering information for the feature.

Table continues…

Problem	Possible Cause	Action
User reports that after setting number using Self Administration for EC500, calls are delivered properly to the cell phone, but there is no office caller ID and he cannot use FNEs.	A dialing prefix or country code was entered as part of the phone number.	Instruct user to separate entry of dialing prefix, country code, and phone number by an asterisk.
User reports some people he calls see an office caller ID and others see the cell phone number.	There are multiple PBXs. Only calls to the PBX where the user is located can see the office caller ID.	Administer SIP signaling groups connecting the PBXs and administer the Mapping Subscriptions form to shared the mappings among the PBXs.

Testing why users cannot receive Extension to Cellular calls

About this task

If Extension to Cellular users cannot receive calls on their cell phones, follow these procedures in the suggested order to isolate and fix the problem. After each step, verify if the problem was fixed. Make a call to the mapped cell phone through the office telephone number.

Procedure

1. Verify that you can call the cell phone from the switch.

   This call also verifies that the service contract with the cellular service provider (CSP) is active, and that the user gets good coverage in that area.

   Make the direct call to the published number of the cell phone. When making this test call, wait until the call rings the cell phone which verifies that there is coverage. Or, wait until the call goes to the cellular voice mail. This test call verifies that the service is provided even when there is weak coverage.

2. Enter `status station`.

   Verify the office number that the Extension to Cellular telephone is mapped to. Verify that SAC or Call Forwarding has not been activated on the principal extension.

3. For the Extension to Cellular extension, enter `status station <extension>`.

   Check the following states:

   - The service state is “in service/idle.” If not, enter `release <extension>` to put the extension back in the active state.
   - The Extension to Cellular state is enabled on the Status Station screen. If Extension to Cellular is disabled, ask the user to enable Extension to Cellular for the principal office number.

4. On the Stations with Off-PBX Telephone Integration screen, verify that the entries in the following fields are correct:

   - Mobility Trunk Group

- Dial Prefix
- Calls Allowed
- Cell Phone Number

5. Check the ARS Analysis table and ensure that there is an entry to route the cell phone number over an ISDN trunk on the switch.
6. If the Mobility Trunk Group is ars or aar, verify that no FAC number is included in the cell phone number field.
7. Enter `list ars route-chosen 1234567890`, where *1234567890* is a 10-digit cell phone number, to verify the type of routing used to route the call.
8. Check ARS digit conversion to verify that no unwanted characters are added to the dial string.

   If the problem cannot be corrected by following this procedure, escalate the issue to Avaya Remote Technical Services (RTS). In addition to the preceding checks, verify with the technician that the Extension to Cellular station can receive incoming calls.

Chapter 92: Facility and Non-Facility Associated Signaling

With Facility Associated Signaling (FAS), an ISDN-PRI T1/E1 interface D-channel can carry signaling information for all the bearer (B) channels on its associated spans.

With Non-Facility Associated Signaling (NFAS), an ISDN-PRI T1/E1 interface D-channel can carry signaling information for as many as 300 bearer (B) channels on its associated spans.

Detailed description of Facility and Non-Facility Associated Signaling

With Facility Associated Signaling (FAS), an ISDN-PRI T1/E1 interface D-channel can carry signaling information for all the bearer (B) channels on its associated spans.

With Non-Facility Associated Signaling (NFAS), an ISDN-PRI T1/E1 interface D-channel can carry signaling information for up to 300 bearer (B) channels on its associated spans. In other words, a single D-channel can carry signaling information for numerous B-channels that are located on different DS1 media modules.

Note:

NFAS is valid for T1/E1 Country Protocol 1 only. Digital T1 service is also sometimes called DS1 to distinguish the service from analog T1 service.

ISDN-BRI trunks do not support NFAS. For more information, see, ISDN Service.

D-channel backup with NFAS

With NFAS, you can administer a backup D-channel to improve reliability. The system switches to the backup D-channel, if a signaling link failure occurs on the primary D-channel span.

You administer one D-channel as the primary D-channel, and another D-channel as the secondary D-channel. These assignments ensure that both D-channels are in the same state at the same time, and that neither channel can be used to carry B-channel traffic at any time. The primary D-channel has precedence over the secondary D-channel.

When D-channel backup is activated, the system preserves all calls that are answered. However, some call-related information can be lost. Calls that are not answered when D-channels are switched, can also lose call-related information.

The following figure shows a possible configuration that involves three ISDN-PRIs between a DEFINITY Server and another DEFINITY Server or the public network.

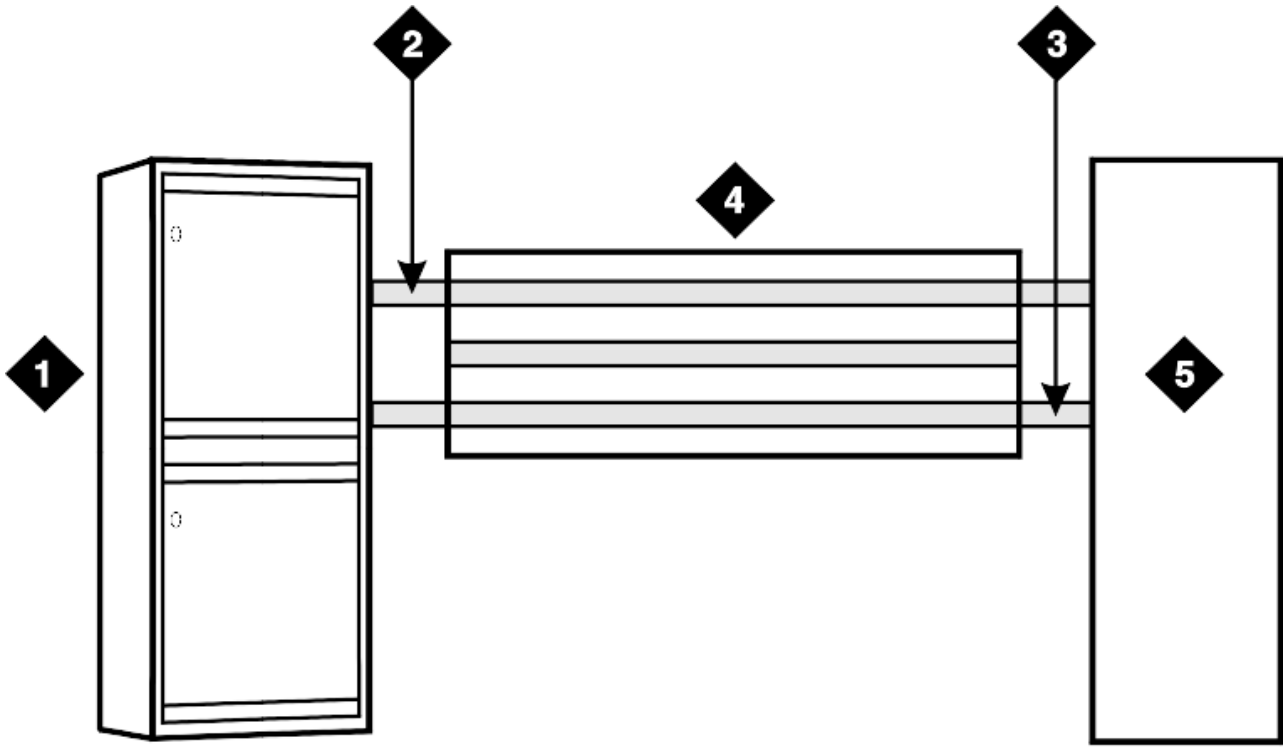


Figure 13: ISDN-PRI configuration

Table 79: Figure notes:

1. Avaya S8XXX Server
2. Secondary D-channel
3. Primary D-channel

1. ISDN-PRI controlled by D-channel
2. Network far-end DEFINITY server

With T1 (24-channel) interfaces, two of the ISDN-PRIs contain a D-channel and 23 B-channels. The other ISDN-PRI contains 24 B-channels. One of the D-channels is the primary D-channel, and the other is the secondary D-channel. Together, this pair of D-channels signals for all 70 (23+24+23) B-channels in the three Primary Rate Interfaces.

Since the D-channels carry signaling for more than one ISDN-PRI facility, D-channel backup requires the use of NFAS. At any given time, one of the two D-channels is carrying Layer 3 signaling messages, while the other D-channel is active at layer 2, but in standby mode only. Any layer 3 messages received over the standby D-channel are ignored. Since only one of the D-channels can be active at a time, the two D-channels cannot share load. The two D-channels

can provide signaling for only a predefined set of B-channels and cannot dynamically back up other D-channels on other interfaces.

D-channel backup activation

D-channel Failure

If the signaling link fails on the active D-channel, D1, or the hardware that carries the D1 channel fails, the system sends a message over the standby D-channel, D2. D2 then becomes the active D-channel and carries all subsequent signaling messages. When the signaling link or the hardware on D1 recovers from the failure, D1 becomes the standby D-channel.

System Technician

If a system technician sends a command to a switch over a D-channel, the system tears down the signaling link on D1. Then, the system sends a message on D2 to request that D2 become the active D-channel. D2 then becomes the active D-channel, and the switchover is complete.

Facility and Non-Facility Associated Signaling administration

The following tasks are part of the administration process for the Facility and Non-Facility Associated Signaling feature:

- Reviewing the guidelines for FAS and NFAS
- Implementing FAS and NFAS

Related links

[Reviewing the guidelines for FAS and NFAS](#) on page 808
[Implementing FAS and NFAS](#) on page 808

Screens for administering Facility and Non-Facility Associated Signaling

Screen name	Purpose	Fields
DS1 Media Module	Define the signaling mode.	Signaling Mode
Processor Channel	Assign processor channels to the link that is administered on the Interface Links screen.	All
Signaling Group	Define the signaling group.	All
Trunk Group	Add trunk ports to the trunk group, and to the signaling group.	• Port • Sig Grp

Reviewing the guidelines for FAS and NFAS

Procedure

1. Decide which T1/E1 facilities use FAS.
2. Decide which of the remaining T1/E1 facilities carry D-channel signaling information on the sixteenth (E1) or the twenty-fourth (T1) channel.

   For those channels that have a D-channel backup, D-channel pairs must be allocated.
3. Define Signaling Groups.

   A Signaling Group is a group of B-channels for which a given D-channel, or D-channel pair, carries the signaling information. Each Signaling Group must be designated as either a FAS or an NFAS Signaling Group.

   - A FAS Signaling Group must contain all the ISDN B-channels on the T1/E1 interface that are associated with the D-channel of the group. An FAS signaling group cannot contain B-channels from any other DS1 media module. For 24-channel DS1 boards, some DS1 ports can use in-band, robbed-bit, signaling and be members in a tie trunk group instead of an ISDN trunk group. These tie trunks cannot be members of a Signaling Group.
   - No restriction exists on which T1/E1 ports can belong to an NFAS Signaling Group. Normally, an NFAS Signaling Group consists of one or two D-channels, and several complete T1/E1 interfaces.
   - If a Signaling Group contains only a subset of the B-channels of a T1/E1 interface (ports 1 to 12, for example), the group is considered to be an NFAS Signaling Group, not an FAS Signaling Group. The remaining B-channels on the T1/E1 interface are then assigned as members of another NFAS Signaling Group.
4. You must assign an Interface ID to each T1/E1 facility in an NFAS Signaling Group.

   For example, if the B-channels in a Signaling Group span three T1/E1 facilities, you must assign a unique Interface ID to each of the three facilities. This designation is required to uniquely identify the same B-channel (port) number on each of the T1/E1 facilities in the Signaling Group. Therefore, this interface must be agreed upon by both sides of the interface, and administered before initialization.
5. Primary and secondary D-channel backup must be agreed by both sides of the interface, and administered before initialization.

   If the IDs do not match, the signaling group comes up, but calls fail.

Implementing FAS and NFAS

Procedure

1. Administer the DS1 Media Module screen.
2. Administer the Interface Link screen and associated screens.

You can administer the Interface Link screen and associated screens any time after you administer the DS1 Media Module screen, with the following restrictions:

- You cannot assign a D-channel on a Signaling Group screen, unless the associated link is disabled.
- You cannot assign a trunk member until you administer the associated Signaling Group.

3. Administer the ISDN-PRI Trunk Group, Signaling Group, and Trunk Group screens.

   The screens in this administration section show the DS1 interface configuration for NFAS.

Administering the DS1 Media Module for FAS and NFAS

About this task

Procedure

You must specify the **Signaling Mode** field for each DS1 media module.

In this mode, either inband robbed-bit signaling, or a D-channel on another DS1 media module. is used to signal all trunks on this media module.

Administering the Trunk Group and Signaling Group for FAS and NFAS

Procedure

1. Note the following details shown in the Signaling Group screen (the figure on page 810, the figure on page 810, and the figure on page 810):
   - Signaling Group 1 B-channels on DS1 boards B0 and B1 are signaled by D-channel pair B1524 (see the **Primary D-Channel** field) and B1624 (see the **Secondary D-Channel** field).
   - Signaling Group 2 B-channels on board B1 are signaled by D-channel B1824.
   - Board B0 has no D-channel. The B-channels on board B0 can be signaled by either D-channel pair B1524/B1624 (Signaling Group 1) or D-channel B1824 (Signaling Group 2).
   - The DS1 interface on board B19 (Signaling Group 3) is a Facility Associated Signaling situation. Note that the system does not display the **Secondary D-channel** and **Trunk Board/Interface ID** fields when the **Associated Signaling** field is set to y.

```
add signaling-group next                                    Page   1 of   5
                                SIGNALING GROUP

 Group Number: 3                 Group Type: isdn-pri
                       Associated Signaling? n          Max number of NCA TSC: 0
                          Primary D-Channel: 1v116      Max number of CA TSC: 0
                        Secondary D-Channel: _______  Trunk Group for NCA TSC: ___
         Trunk Group for Channel Selection: ____     X-Mobility/Wireless Type: NONE
       TSC Supplementary Service Protocol: a          Network Call Transfer? n

          Trunk Brd       Interface ID          Trunk Brd       Interface ID
           1: 2v5__          0__               11: _____           __
           2: _____          __                12: _____           __
           3: _____          __                13: _____           __
           4: _____          __                14: _____           __
           5: _____          __                15: _____           __
           6: _____          __                16: _____           __
           7: _____          __                17: _____           __
           8: _____          __                18: _____           __
           9: _____          __                19: _____           __
          10: _____          __                20: _____           __

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

Figure 14: Signaling Group screen (Group 1) - D-channel backup, three DS1 interfaces

```
                              SIGNALING GROUP

Group Number : 2    Associated Signaling? n          Max number of NCA TSC: 0
                       Primary D-Channel: 1B1824     Max number of CA TSC: 0
                     Secondary D-Channel: ______  Trunk Group for NCA TSC: __
       Trunk Group for Channel Selection: _____
    Trunk Brd    Interface ID        Trunk Brd    Interface ID
  1:   1B17          0             11:   ____          __
  2:   1B18          1             12:   ____          __
  3:   ____          __            13:   ____          __
  4:   ____          __            14:   ____          __
  5:   ____          __            15:   ____          __
```

Figure 15: Signaling Group screen (Group 2) - no D-channel backup, two DS1 interfaces

```
                              SIGNALING GROUP

Group Number : 3     Associated Signaling? y       Max number of NCA TSC: 0
                        Primary D-Channel: 1B1924  Max number of CA TSC: 0
                                                Trunk Group for NCA TSC: __
       Trunk Group for Channel Selection: _____
```

Figure 16: Signaling Group screen (Group 3) - FAS

2. In the **Sig Grp** column on the Signaling Group Screen perform the following actions:
   - If the system displays a DS1 interface in only one Signaling Group, leave the **Sig Grp** field blank. The system automatically populates the field with the correct Signaling Group.
   - If the system displays a DS1 media module in more than one Signaling Group, type the Signaling Group numbers in the appropriate fields.
3. Press `Enter` to save your changes.

Chapter 93: Facility Restriction Levels

Use the Facility Restriction Levels (FRL) feature to restrict some types of calls to specific users. For example, you can use FRL for some users to place international calls, but for other users to place only local calls.

Facility Restriction Levels supports the following capabilities:

Alternate Facility Restriction Levels (AFRL)

Use AFRL to assign a second set of FRLs within a route pattern or to lines and trunks. For example, you can use an AFRL to disable the ability to place long distance calls when the office is closed.

Traveling Class Mark (TCM)

The system uses TCM to pass the FRL of a caller from one server to another server. The server that receives the FRL uses the FRL to determine the calling privileges that are assigned to the user.

Detailed description of Facility Restriction Levels

The FRL controls the privileges of the call originator. The system compares the FRL of the call originator with the FRL of the call termination point. The system can continue the call if the FRL of the call originator is equal to or greater than the FRL of the:

- Trunk group that is the terminating point of a call that is not an Automatic Alternate Routing (AAR) or an automatic route selection (ARS) call
- Route pattern that is assigned to the trunk that is the terminating point of an AAR or an ARS call

AAR and ARS calls with Facility Restriction Levels

Originators of AAR and ARS calls with Facility Restriction Levels

An originator of an AAR or an ARS call can be:

- An attendant
- A telephone user
- A remote access user
- A data terminal with a keyboard

- An incoming tie trunk group from a subtending location
- An incoming intertandem tie-trunk group, at a server or a switch
- An incoming access tie trunk group that links a remote main server or a switch to a tandem server or a switch

When the system determines the FRL of the call originator, the system uses the FRL that is assigned to the COR of:

- A telephone user
- All incoming tie trunk groups
- An attendant group for attendant-extended calls
- The individual attendant, if Individual Attendant Access is assigned
- The data module that is associated with a data terminal
- The barrier code that a user dials for a remote access call

  If the remote access call does not require a barrier code, no FRL exists.

Call termination points for AAR and ARS calls with Facility Restriction Levels

A termination point for an AAR or an ARS call can be:

- A tie trunk
  - A tie trunk termination point for an AAR and ARS call can include a common-control switching arrangement (CCSA) access trunk and an enhanced private switched communications services (EPSCS) access trunk.
  - A tie trunk termination point for an AAR and ARS call excludes a release-line trunk (RLT).
- A Wide Area Telecommunications Services (WATS) trunk
- A central office (CO) trunk
- A foreign exchange (FX) trunk
- An integrated services digital network-primary rate interface (ISDN-PRI) trunk

Each of these outgoing trunk groups has a COR that contains an FRL. However, for AAR and ARS calls, the system uses the FRL that you assigned to the route pattern of the trunk group.

Alternate Facility Restriction Levels

Use the Alternate Facility Restriction Levels (AFRL) capability to define a second set of facility restriction levels within a route pattern, or for lines or trunks. Attendants and system administrators can activate the AFRLs and change user access to lines and trunks. For example, you can use AFRL to disable the ability to place a long distance call when the office is closed.

AFRL alters the route patterns for originating telephones, originating trunks, and dialed authorization codes. If AFRL is active:

- Traveling Class Mark (TCM) is set to a new FRL value
- The TCM information that the system records in the Call Detail Recording (CDR) records is the value of the AFRL, not the original TCM.

Caution:

AFRL has an impact on both AAR and ARS call routing because AFRL can change routing preferences. The use of AFRL on tandem and tie-trunk applications can affect entire networks. The system can block calls that are part of a cross-country private network that need to be routed further.

Alt-frl feature button

You can assign an **alt-frl** button to any attendant console and to any user telephone. The attendant or the user presses the **alt-frl** button to activate and deactivate the AFRL. The use of the **alt-frl** button can affect the status of other buttons.

When AFRL is active, the user might notice a change in calling privileges. Consider notifying users of the changes in calling privileges, and prepare your telecommunications department to respond to user inquiries.

Authorization codes and Facility Restrictions Levels

Authorization codes prevent unauthorized access to some system facilities. When a user dials an authorization code, the system checks the code. If the code is invalid, the system generates the intercept tone. If the code is valid, the system uses the COR and the FRL that is associated with the authorization code for further call processing. However, if AFRL is activated, the system uses the AFRL for further call processing.

If the system uses an intertandem tie trunk group for a call, the system outpulses a TCM as the last digit of the number. If the FRL of the intertandem tie-trunk is equal to or greater than the terminating FRL, the system proceeds with call processing. If the FRL of the originator is less than the FRL of the termination point, the system compares the TCM with the FRL of the tie trunk. If the TCM is greater than or equal to the FRL of the tie trunk, the system proceeds with call processing.

Facility Restriction Levels administration

This section describes the screens for the Facility Restriction Levels feature.

Screens for administering Facility Restriction Levels

Screen name	Purpose	Fields
AAR Digit Analysis Table	Associate a dialed string with a route pattern, and thus to an FRL.	Route Pattern
ARS Digit Analysis Table	Associate a dialed string with a route pattern, and thus to an FRL.	Route Pattern
Attendant Console	Assign an **alt-frl** button for the attendant so that the attendant can activate the AFRL capability.	Any available button field in the **Feature Button Assignments** area
	Assign a COR for the attendant to associate an FRL with the attendant.	COR
Class of Restriction	Assign an FRL to the Class of Restriction (COR).	FRL
Console Parameters	Assign a COR for the attendant group to associate an FRL with the attendant group.	COR
Data Module	Assign a COR for the data module to associate an FRL with the data module.	COR
Remote Access	Assign a COR to the barrier code to associate an FRL with the barrier code.	COR
Route Pattern	Assign an FRL to the trunk group.	FRL
Station	Assign an **alt-frl** button for a user so that the user can activate the AFRL capability.	Any available button field in the **Button Assignments** area
	Assign a COR for the user to associate an FRL with the user.	COR
Trunk Group	Require that a user enter an authorization code, if the user wants to tandem a call through an Automatic Alternate Routing (AAR) or an Automatic Route Selection (ARS) route pattern.	Auth Code
	Assign a COR for the trunk group to associate an FRL with the trunk group.	COR

End-user procedures for Facility Restriction Levels

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Using Alternate Facility Restriction Levels

Procedure

1. To activate AFRL, press the **alt-frl** button.
2. To deactivate AFRL, press the **alt-frl** button.

Considerations for Facility Restriction Levels

This section provides information about how the Facility Restriction Levels (FRL) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Facility Restriction Levels under all conditions. The following considerations apply to Facility Restriction Levels:

Trunk groups

- Use the Route Pattern screen to assign the FRL to a trunk group.
- You can use the same trunk group in more than one route pattern.
- The same trunk group can have a different FRL in a different pattern.
- You can assign the same FRL to more than one trunk group.

General access

Be consistent in FRL assignments. Always use FRL 0 or FRL 1 for a trunk group that everyone can access.

Route patterns

If you use a range of 0 through 5 in one route pattern, use the same range in another pattern, if all users can access the first-choice route.

Assign a Class of Restriction (COR) with an FRL of 0 to a group of users to restrict the users to local calls. Use any other number for the FRL on your first-choice route pattern.

Remote access barrier codes

You assign FRLs for remote access users through the remote-access barrier codes. The simplest way to assign these FRLs is to duplicate the on-premises FRLs, and then relate the appropriate barrier code to users who use remote access. For more information, see Remote Access.

Related links

Remote Access on page 1164

Interactions for Facility Restriction Levels

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

- Call Detail Recording (CDR)

  If your system uses a 15-digit CDR account, the system overwrites the **FRL** field in the CDR record with the account code.

Chapter 94: Facility Test Calls

Use the Facility Test Calls feature to make test calls to access specific trunks, dual-tone multifrequency (DTMF) receivers, time slots, and system tones.

Detailed description of Facility Test Calls

With the Facility Test Calls feature, you can make test calls to access specific trunks, dual-tone multifrequency (DTMF) receivers, time slots, and system tones.

You can make test calls from any telephone to test specific trunks. Avaya maintenance personnel can make test calls from remote locations.

The system supports four types of facility test calls.

- Trunk test for specific tie trunks or central office (CO) trunks.

  You cannot test direct inward dialing (DID) trunks with this feature. You can use your Class of Restriction (COR) to use the Facility Access Trunk Test function.
- System tone test for a specific system tone.

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

You can create a Feature Access Code (FAC) for administrators and users to access the Facility Test Calls feature. You can also assign a feature button for a user to access the feature from the user telephone.

Facility Test Calls security

Security alert:

Proper administration of Facility Test Calls minimizes the ability of unauthorized persons to gain access to your system. However, you are responsible to properly implement the feature, evaluate and administer the various restriction levels, protect access codes, and distribute the codes only to individuals who are aware of the sensitive nature of the access information. Instruct each authorized user to properly use access codes.

In rare instances, unauthorized individuals use Facility Test Calls to connect to the public network. Applicable tariffs require that you pay all network charges for such calls. Avaya LLC cannot be

responsible for charges incurred by such calls, and will not make any allowance or give any credit for charges that result from unauthorized access.

To help secure the Facility Test Calls feature from unauthorized use:

- Remove the access code when the access code is unused.
- Change the access code from the default value that is set when you receive your system.
- Secure records of the access code.
- Use COR to restrict the number of users who can use the access code.

You can set Logoff Notification to notify you when you log off the system that the Facility Test Calls feature is still enabled. This notification can alert you that an unauthorized activation of the feature has occurred.

Administering Facility Test Calls

This section describes the screens for the Facility Test Calls feature.

Screens for administering Facility Test Calls

Screen name	Purpose	Fields
Class of Restriction	Assign an FRL to the Class of Restriction (COR).	FRL
Feature Access Code (FAC)	Specify a Feature Access Code (FAC) for Facility Test Calls	Facility Test Calls Access Code
Station (multiappearance)	Assign a trk-ac-alm facility test lamp alarm button for a user.	Any available button field in the **Button Assignments** area

Considerations for Facility Test Calls

This section provides information about how the Facility Test Calls feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Facility Test Calls under all conditions. The following considerations apply to Facility Restriction Levels:

- You must use a digital telephone that resides on the local server to make test calls.

Interactions for Facility Test Calls

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

Service Observing

You cannot use Facility Test Calls for Service Observing.

Chapter 95: Fax over IP

With the Fax over IP feature, enterprise networks interoperate with PSTN networks to transfer faxmessages over IP. Only the G430 and G450 gateways support the Fax over IP feature. Fax over RTP/SRTP is only supported by G450 using DSP of type MP160, or G430 with MP12 or 40 channel on board.

Related links

Detailed description of Fax over IP on page 821

Detailed description of Fax over IP

Communication Manager supports the transition of an existing SIP audio call to a fax call.

During a SIP audio call, when Communication Manager receives a reINVITE message with the audio and image stream, Communication Manager performs one of the following operations:

- If T.38 is administered, Communication Manager accepts the image stream and rejects the audio stream.
- If T.38 is not administered, Communication Manager accepts the audio stream and rejects the image stream.

The gateway at the near end converts the analog fax streams into T.38-defined data packets. The gateway at the far end converts the T.38-defined signals into analog fax streams and transmits the streams to the receiving analog device.

Communication Manager uses the T.38 protocol for fax transmission only if the protocol can be successfully negotiated with the peer SIP entity. Otherwise, Communication Manager falls back to G.711 for fax transmission if the G.711 codec is administered.

Related links

Fax over IP on page 821

Fax over IP administration

Screens for administering Fax over IP

Screen name	Purpose	Fields
IP Codec set	Administering the **Fax over IP** feature	**FAX Mode** **ECM** **XMT**

Related links

Fax over IP on page 821

Administering Fax over IP

About this task

Use this procedure to administer the **Fax over IP** feature.

Procedure

1. Type `change ip-codec-set n`, where *n* is the Codec Set number.
2. On page 2 of the IP Codec Set screen, set the **FAX Mode** field to t.38fallback, t.38-standard, pass- through.

   The system displays the **ECM** field. If the mode is t.38fallback, the **XMT** field can be used to select 'udptl' or 'rtp'.
3. To enable the error correction mode, set the **ECM** field to `y`.

   The default value for the **ECM** field is n.
4. Save the changes.

Related links

Fax over IP on page 821

Chapter 96: Feature Access Codes

Use Feature Access Codes (FAC) to provide users with quick access to certain features of the telephone system. When you assign a FAC to a feature, users do not have to program a button on the telephone to use this feature. Instead, users just dial the FAC.

Detailed description of Feature Access Codes

A Feature Access Code (FAC) must contain from one to four characters. These characters can be digits or a combination of digits and a character such as an asterisk (*) or a pound sign (#). If you use a character, you must position this character first in the FAC.

The asterisk (*) and pound sign (#) characters are often used in pairs. You can use one of these characters and digits to activate a feature and the other character and the same digits to deactivate the feature. For example, if you use the asterisk (*) and the digits 2 and 9 to activate the Posted Messages feature, then you can use the pound sign (#) character and the digits 2 and 9 to deactivate the Posted Messages feature.

Note:

Users with analog rotary telephones cannot dial FACs that contain an asterisk (*) or a pound sign (#).

You can use the following types of FACs:

- Access FACs: To gain access to a feature.
- Activate or deactivate FACs: To activate or deactivate a feature.
- Send or Cancel FACs: To send or cancel a message.
- Lock or unlock FACs: To lock or unlock the message retrieval capability of a telephone.

Many features have default FACs that you can change.

An FAC must be unique and must conform to the dial plan. If you define an FAC that is assigned to another feature, the system displays an error message.

Note:

If a feature such as Call Forwarding, Send All Calls, EC500, or Limit Number of Concurrent Calls is activated or deactivated on a deskphone by using an FAC, but the corresponding feature button is not administered on the deskphone, an indication of feature activation or

deactivation is not provided to the user. Therefore, Avaya recommends assigning a feature button to the deskphone of the user who intends to use the feature.

Feature Access Codes administration

The following tasks are part of the administration process for the Feature Access Codes feature:

- Assigning Feature Access Codes
- Changing or deleting Feature Access Codes

Related links

Assigning Feature Access Codes on page 824
Changing or deleting Feature Access Codes on page 825

Preparing to administer Feature Access Codes

Procedure

Ensure that Feature Access Codes are set up in your dial plan.

You must have a FAC or Deactivation Access Code (DAC) entry on the dial plan screen for the digit range that you intend to use for you Feature Access Codes. For a description of how to set up your dial plan, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Feature Access Codes

Screen name	Purpose	Fields
Feature Access Code (FAC)	Assign FACs to specified telephone features.	All

Assigning Feature Access Codes

Procedure

1. Enter `change feature-access-codes`.
2. In the field next to the specific feature to which you want to assign the FAC, type a FAC that conforms to your dial plan.

   You might have to scroll through several pages of the Feature Access Code (FAC) screen to find the telephone feature that you want.

   Some features require more than one FAC. Type a FAC in each required field. For example, type a separate FAC in the **Call Forwarding Activation Busy/DA** field, the **All** field, and the **Deactivation** field.
3. Press `Enter` to save your changes.

4. Ensure that you notify all users about the assigned FACs.

Changing or deleting Feature Access Codes

Procedure

1. Enter `change feature-access-codes`.
2. In the field next to the feature that you want to change, type a new FAC that conforms to your dial plan over the existing FAC.

   You might have to scroll through several pages of the Feature Access Code (FAC) screen to find the telephone feature that you want.

   Some features require more than one FAC. type a FAC in each required field. For example, type a separate FAC in the **Call Forwarding Activation Busy/DA** field, the **All** field, and the **Deactivation** field.
3. To remove a FAC, delete the existing FAC and leave the field blank.
4. Press `Enter` to save your changes.
5. Ensure that you notify all users about the changed FACs.

Feature Access Codes troubleshooting

This section lists the known or common problems that users might experience with Feature Access Codes:

Problem	Possible cause	Action
The user experiences delays when the user attempts to use a FAC.	You might have a FAC and an extension with the same digits on your dial plan.	Check your dial plan to see if you have a FAC and an extension with the same digits. For more information, see *Administering Avaya Aura® Communication Manager*.

Chapter 97: Group Paging

Use the Group Paging feature to make an announcement over a group of digital speakerphones.

- You can create up to 32 paging groups on one media server.
- Each group can consist of up to 32 extensions.
- You can assign the same extension to different groups.

Detailed Description of Group Paging

With the Group Paging feature, you can create a page group, and assign extensions as members of the group. You assign an identifying extension to each page group, which users dial to page the group. When a user dials the extension of the paging group, Communication Manager activates the speakers on all the telephones in the group. Speakerphone paging is one-way communication: Group members hear the person place the page, but cannot respond directly.

The Group Paging feature now supports SIP phones. SIP phones not only originate a group page but also become a part of the paging group. The behavior of non-SIP phones remains unchanged.

Group Paging restrictions

Pages are not always heard on every telephone in a group. An extension does not transmit a group page if the extension has an active or a ringing call, or if the extension is off-hook. Listeners can drop a page if the listeners disconnect. Pages cannot be heard when the Send All Calls or Do Not Disturb features are activated.

When a group member does not hear the announcement for any of these reasons, the caller is not notified. Therefore, the originator of an important page might want to check with the group members to ensure that all members heard the page.

Control of access to paging groups

Each paging group is assigned a class of restriction (COR). Thus you can provide or deny access to different classes of users by setting calling permissions appropriately. Note that you can administer CORs so that remote callers can make speakerphone pages. If you do not want to allow remote users to page, you can use the Class of Restriction screen to set calling permissions for vector directory numbers (VDNs) and trunk groups so that neither can initiate pages. For more information on CORs, see Class of Restriction.

Group Paging administration

The following tasks are part of the administration process for the Group Paging feature:

- Creating a paging group
- Changing a paging group
- Viewing all paging groups

Related links

Creating a paging group on page 827
Changing a paging group on page 828
Viewing all paging groups on page 828

Screens for administering Group Paging

Screen Name	Purpose	Fields
Group Paging Using Speakerphones	Create or change a paging group, and add or delete group members.	All
Speakerphone Page Groups	View a list of all existing paging groups.	All

Creating a paging group

Procedure

1. Enter `add group-page` *n*, where *n* is a number between 1 and 32, or type `add group-page next` for the next available group number.
2. In the **Group Extension** field, type the extension that users dial to page the members of this group.
3. In the **Group Name** field, type the name that you want to assign to this paging group.

   The telephone screen of the caller displays this name when paging the group.
4. In the **COR** field, type the Class of Restriction (COR) that you want to assign to this group.

   Any user who wants to page this group must have permission to call this COR.
5. In the **Ext** field in row 1, type the extension of the first member of the paging group.
6. Type the remaining extensions of the other members of this group.

   When you save your changes, the software automatically completes the **Name** fields with the names that are associated with the extensions on the Station screen.
7. Set the **Alert** field to `y` for telephones that require an alert message to ring for an inbound call from a group page number. For example, Spectralink wireless telephones.
8. Save the changes.

   Paging is now active on the system.

Changing a paging group

About this task

You can add or delete members of a paging group, or modify the other attributes of the group, such as the group name, group extension, or COR.

Procedure

1. Enter `change group-page n`, where *n* is the number of the paging group that you want to change.
2. In the **Ext** field, type the extension of a member that you want to add, or delete the extension of a member that you want to remove from the group.
3. Make the required changes in any of the following fields:
   - **Group Name**
   - **Group Extension**
   - **COR**
   - **Alert**

Viewing all paging groups

Procedure

Enter `list group-page`.

If there are more page-groups, click **Next**.

Considerations for Group Paging

This section provides information about how the Group Paging feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Group Paging feature under all conditions.

- The person making the group call should wait until after hearing the zip tone before starting to speak.

Interactions for Group Paging

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

Attendant Intrusion

Attendants cannot intrude on group pages. If the attendant tries to intrude on the originator of the page, the intrusion attempt succeeds. However, all group page members can hear both the paging originator and the attendant.

Auto Exclusion and Manual Exclusion

Bridged appearances are not allowed on the page. Therefore, the Auto Exclusion and the Manual Exclusion features are disabled. Auto Exclusion is disabled because there are no bridged appearances to alert when the page terminates.

Auto Hold

Auto Hold does not put a group page on hold. The page is dropped, and the incoming call is answered.

Automatic Callback

Automatic Callback is disabled when a user calls an active page group.

Bridging

Bridging is disabled on this feature. A bridged appearance of a group member does not receive any indication of a call when the page arrives. The bridged appearance cannot bridge onto the page.

Call Coverage

Pages do not follow the coverage paths of the group members. A page group cannot be a coverage point.

Call Park

Group members who receive a page cannot park the call.

Call Pickup and Direct Call Pickup

Other extensions cannot pick up a group page.

Call Forwarding

Group pages cannot be forwarded.

Conference

Neither group members who receive a page, nor the originator of the page, can conference the page to other extensions.

Distributed Communications System (DCS)

Page groups cannot be administered across DCS servers or switches. DCS is not supported.

Do Not Disturb

If a member of a page group activates Do Not Disturb, that member does not receive pages.

Go to Cover

The Go to Cover feature is ignored because group pages do not follow coverage.

Hold

The originator of a group page can put the page on hold, but group members cannot.

Leave Word Calling

Leave Word Calling (LWC) is disabled. A page group cannot receive messages.

Manual Signaling

The Manual Signaling feature cannot be assigned to a page group.

Send All Calls (SAC)

If a member of a page group activates SAC, that member does not receive pages.

Service Observing

Group page members and page originators cannot be observed while active on a page.

Transfer

Group members cannot transfer a page.

Trunks

Trunks cannot be added to a page group.

Vectoring

Paging groups cannot be explicitly added to a vector path.

Group Paging troubleshooting

This section lists the known or common problems that users might experience with the Group Paging feature.

Problem	Possible cause	Action
A user gets a busy signal when the user tries to page.	All telephones in the group are busy or off-hook.	Wait a few minutes and try again.
	Send All Calls or Do Not Disturb is activated for all telephones in the group.	Group members must deactivate these features to hear a page.
Some group members do not hear a page.	Send All Calls or Do Not Disturb is activated for the telephones of these group members.	Group members must deactivate these features to hear a page.

Chapter 98: Hold

Use the Hold feature to temporarily disconnect from a call, use the telephone for another call, and then return to the original call.

Detailed description of Hold

Multiappearance telephone users can use a Hold button to activate Hold. With Automatic Hold, a user can also press a second call appearance to put an active call on hold. The system holds the call at the call appearance that is used for the call. Multiappearance telephone users can hold a call on each call appearance.

Single-line and multiappearance telephone users can use two types of Hold, Soft Hold and Hard Hold.

Soft Hold

Use Soft Hold to conference or transfer a call that includes the held call. With Soft Hold, the user can put a call on hold, consult with another party, activate or deactivate a feature, and then return to the call on hold.

Single-line telephone users flash the switch hook, and Multiappearance telephone users press the conference button or the transfer button to place a call on Soft Hold.

Hard Hold

Use Hard Hold to perform operations that do not include the held call. The user can put a call on hold and call another party. The user can then answer a waiting call, transfer or conference the waiting call, or activate or deactivate features.

Single-line telephone users flash the switch hook, and Multiappearance telephone users press the hold button or use automatic hold to place a call on Hard Hold.

Automatic Hold

With Automatic Hold, attendants and multifunction telephone can alternate easily between two or more calls. For example, when an attendant or a multifunction telephone user selects a second call, the system automatically puts the active call on hold, and makes the second call active. Automatic Hold is a system-wide capability. If you do not enable Automatic Hold for your system,

the system drops the current active call when an attendant or a user selects a second call. A call that is placed in Automatic Hold is in Hard Hold.

To put an active call on hold, without pressing the **Hold** button, the user presses a second call-appearance button. The second call appearance becomes active. A user can place more than one call on hold. However, the user must keep one call appearance available for other calls.

The controlling telephone can have only one auto-held call on soft hold at a time. A soft hold is the state of a line after the user presses a conference button or a transfer button, but before either process is complete. The controlling telephone is guaranteed the ability to reenter any auto-held call later, unless the auto-held parties disconnect, or the auto-held tone exceeds the auto-held tone time limit.

Hold administration

The following tasks are part of the administration process for the Hold feature:

- Enabling Automatic Hold
- Assigning a FAC for CAS remote hold and answer

Related links

Enabling Automatic Hold on page 832
Assigning a FAC for CAS remote hold and answer on page 833

Screens for administering Hold

Screen name	Purpose	Fields
Feature Access Code (FAC)	Define the Feature Access Code (FAC) for centralized attendant services (CAS) attendant remote hold and answer.	CAS Remote Hold/Answer Hold-Unhold
Feature-Related System Parameters	Enable the Automatic Hold capability for your system.	Auto Hold

Enabling Automatic Hold

Procedure

1. Enter `change system-parameters features`.
2. Click **Next** until you see the **Auto Hold** field.
3. In the **Auto Hold** field, perform one of the following actions:
   - If you want the Automatic Hold capability available to all users on your system, type `y`.
   - If you do not want the Automatic Hold capability available to any users on your system, type `n`.

4. Press `Enter` to save your changes.

Assigning a FAC for CAS remote hold and answer

Procedure

1. Enter `change feature-access-codes`.
2. In the **CAS Remote Hold/Answer Hold-Unhold Access Code** field, type the FAC that a CAS attendant can use to:
   - Place calls on hold
   - Answer calls that are held at a remote server that is running Communication Manager.
3. Press `Enter` to save your changes.

Considerations for Hold

This section provides information about how the Hold feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Hold under all conditions. The following considerations apply to Hold:

- To drop a call that is dialed from a single-line telephone within the first 10 seconds after you complete dialing the call, flash the switch hook.
- A single-line telephone user cannot hold a call that involves an attendant. A multiappearance telephone user can hold a call that involves an attendant, unless the user attempts to conference or transfer the call.
- When only Automatic Hold is involved, and the attendant on an active loop presses a second loop, the system places the active call on Hard Hold.
- The Held Call Timed Reminder does not apply to conference calls, and is not started when a conference is placed on hold.
- Automatic Hold operates in conjunction with the START key or the Automatic Start feature of an attendant console. The START key and the Automatic Start operation have precedence over Automatic Hold, and place an active loop call on soft hold.

Interactions for Hold

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

Automatic Callback

A single-line telephone user cannot receive an Automatic Callback call while a call is on hold.

Bridged Call Appearance

Any user, who is active on a bridged call, can place the call on hold. If no other users with a bridged call appearance of the same extension are connected to the call, the status lamp at the Bridged Appearance button indicates that the call is on hold. If the primary extension or another bridged appearance is connected to the call, the status lamp at all bridged appearances indicates an active status for the call.

Centralized Attendant Service (CAS)

Automatic Hold does not affect the operation of CAS

Distributed Communications System (DCS)

Automatic Hold does not affect the operation of DCS, and is administered separately for each node in a DCS network.

Leave Word Calling (LWC)

A multiappearance telephone user who is on hold can activate LWC toward the holding user.

A single-line telephone user cannot activate LWC toward another user while a call is on Soft Hold.

Music-on-Hold

Communication Manager does not play music to a held multiparty call.

Personal Central Office Line (PCOL)

When a user, who is active on a PCOL call, puts the call on Hold, the lamp flutters or winks. The status lamp that is associated with the PCOL button lamp does not track the busy or idle status of the PCOL.

Priority Calling

Users can receive priority ringing and have a call on soft hold.

Chapter 99: Hot Line Service

Use the Hot Line Service feature to assign a specific destination to which the user of a single-line telephone automatically connects to a destination when the user goes off-hook.

Detailed description of Hot Line Service

With the Hot Line Service, the user of a single-line telephone can automatically connect to a preassigned destination when the user goes off-hook. You can assign the following numbers as a Hot Line Service destination:

- An attendant
- An extension
- A Feature Access Code (FAC)
- A public telephone number
- A private telephone number

The Hot Line Service destination number must be stored in an Abbreviated Dialing list. When the user goes off-hook, the system automatically routes the call to the stored number, and completes the call as if the user dialed the call.

If an attendant number is the Hot Line Service destination number, the system automatically routes the telephone user to the attendant.

If the appropriate FAC is stored with the number in the Abbreviated Dialing list, the system uses Automatic Alternate Routing (AAR), automatic route selection (ARS), Data Privacy, or Priority Calling.

If the Public Network Access code or the Private Network Access code is the number stored in the Abbreviated Dialing list, the system connects the user to the outside number.

A Direct Department Calling (DDC), a Uniform Call Distribution (UCD), a Terminating Extension Group (TEG) extension, or any individual extension within such a group, can be a Hot Line Service destination.

Hot Line Service retains the way that a user receives calls. Calls to a user with Hot Line Service are controlled by the Class of Restriction (COR) that you assign to the user extension. Hot Line Service does not affect the recipient of the call.

Hot Line Service administration

This section describes the screens that you use to administer the Hot Line Service feature.

- Screens for administering Hot Line Service

Screens for administering Hot Line Service

Screen name	Purpose	Fields
Abbreviated Dialing List • System List • Group List • Personal List	Store the number that you want the system to use when the user enters the dial code.	Dial Code
Data Modules • Data Line Module • MPD/MTDM • Netcon Data Module • Processor Interface Data Module • System Port Data Module • Packet Gateway (PGATE) • Netcon Data Module	Specify Hot Line Service information for the data module.	• Special Dialing Option • Hot Line Destination
Station - single-line	Specify Hot Line Service information for the user.	• Hot Line Destination - Abbreviated Dialing List Number • Hot Line Destination - Dial Code • Special Dialing Code

Considerations for Hot Line Service

This section provides information about how the Hot Line Service feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Hot Line Service under all conditions. The following considerations apply to Hot Line Service:

- Specify the attendant as the Hot Line Service destination when you want the attendant to screen call originations.
- You can assign Hot Line Service to any number of telephones, with the same or different destinations. The number of users who can use Hot Line Service is limited by the number of entries that you can store in the Abbreviated Dialing lists.

- A Hot Line Service user can activate any feature, but only if the FAC is stored in the Abbreviated Dialing List.

Interactions for Hot Line Service

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

Night Service

When Night Service is active, the system redirects the Hot Line Service call.

Bridged Call Appearance - Single-Line Voice Terminal

A bridged call appearance of a telephone that is administered for Hot Line Service, also places a hot line call automatically when a user goes off-hook on that bridged appearance.

Loudspeaker Paging Access

You can use Loudspeaker Paging Access with Hot Line Service to provide automatic access to paging equipment.

Ringback Queuing

If a Hot Line Service call accesses a trunk group with Ringback Queuing, the call can queue, unless the telephone is Termination Restricted by the Class of Service (COR). Queuing, when applicable, is automatic on single-line telephones.

Chapter 100: Hunt Groups

Use the Hunt Groups feature to set up a group of extensions that can handle multiple calls to a single telephone number. You can choose the call distribution method to route calls. For each call to the number, the system hunts for an available extension in the hunt group, and connects the call to that extension.

A hunt group is especially useful when you expect a high number of calls to a particular telephone number. A hunt group might consist of people who are trained to handle calls on specific topics. For example, the group might be a:

- Benefits department within your company
- Service department for products that you sell
- Travel reservations service
- Pool of attendants

A hunt group might also consist of a group of shared telecommunications facilities. For example, the group might be a:

- Modem pool
- Group of data-line circuit ports
- Group of data modules

Detailed description of Hunt Groups

Hunt groups are of two types.

- Small hunt group: supports up to 99 extensions
- Large hunt group: supports up to 8000 extensions

The small hunt group extensions are of two digits, and the large hunt group extensions are of four digits.

Announcements for hunt groups

When an extension is not immediately available, the system plays a recorded announcement to the caller. You can record and assign one delay announcement to each hunt group queue. An

announcement can be shared among hunt groups. Usually, a hunt group announcement asks the caller to wait, and says that the call will be answered in the order in which the call was received.

A call that connects to a delay announcement remains in a queue while the system plays the announcement. If the call is not answered by the time that the announcement completes, the caller hears music, if music is administered. If music is not administered, the caller hears silence. When the call starts ringing at the telephone of a hunt group member, the caller hears ringing.

Delay announcement intervals for hunt groups

You can define a delay announcement interval for each hunt group. This interval of 0 to 99 seconds specifies how long a call remains in the queue before the system connects the call to a recorded announcement. When a call enters the queue, the interval starts. If Call Coverage is administered, the Don't Answer interval of 1 to 99 ringing cycles also starts when the call enters the queue. After these intervals start, one of the following processes also starts:

- If the Don't Answer interval expires before the delay announcement interval expires, the system redirects the call to coverage.
- If no coverage point is available, the call remains in the queue. The system connects the call to the delay announcement when the delay announcement interval expires.
- If the delay announcement interval expires before the Don't Answer interval, the system connects the call to a delay announcement. If the announcement is already in use, the system resets the delay announcement interval.

This process continues as above until the call is answered, goes to coverage, connects to an announcement, or ends because the caller has disconnected the call.

If you set the delay announcement interval to 0 seconds, the system automatically connects a call to the announcement. This announcement is called a forced first announcement. In this case, the system does not connect the call to a hunt group member until after the announcement. The caller does not hear music.

If the system uses call coverage to redirect a call to another hunt group, the caller does not hear the forced first announcement of either hunt group. However, the caller might hear the first or the second announcement of the covering hunt group.

Analog, aux-trunk, or integrated delay announcements for hunt groups

Delay announcements can be analog, aux-trunk, or digitally integrated. For an analog or aux-trunk announcement, a caller who enters the queue hears the associated announcement the next time that the system plays the announcement. A caller who enters the queue after the announcement starts does not hear the announcement until the announcement starts again. For an integrated announcement, multiple callers can be connected to the same announcement at different times, depending on the available ports.

Example

Assume that a hunt group has the following parameters:

- The queue length is 10 calls.

- The queue warning level is 5 calls.
- The recorded announcement delay is 20 seconds.

All hunt group members are busy. A call enters the queue as the fifth call, which causes the queue warning-level lamp to light. Hunt group members see the lamp, and try to quickly complete their current calls. Meanwhile, the call waits in the queue for 20 seconds, and the system plays the recorded announcement. When a hunt group member becomes available, the first call in the queue connects to that group member. The queue warning-level lamp turns off when the number of calls in the queue falls to four.

Call Coverage for hunt groups

You can set up call coverage for a hunt group. Then if a hunt group queue is full, the system sends new calls to the coverage point.

You can specify one of the following methods to determine how the system distributes calls to members of the hunt group:

- Direct Department Dialing (DDD)
- Uniform Call Distribution (UCD)
- Circular
- Automatic Call Distribution (ACD)
- Expert Agent Selection (EAS)

If a call goes into a hunt group queue, the call stays in the queue for the Don't Answer interval. The system then redirects the call to the coverage point. A call coverage point can be another hunt group.

For more information on setting up call coverage, see *Administering Avaya Aura® Communication Manager*.

Call Distribution methods for hunt group types

The system can use different types of station hunting methods to distribute calls to hunt groups. You can specify the call distribution method in the **Group Type** field on the Hunt Group screen. The available values for the **Group Type** field depend on how your system is configured.

You have more call distribution options if you activate the Automatic Call Distribution (ACD) or Expert Agent Selection (EAS) setting. These options are available if the **ACD** and **Expert Agent Selection (EAS)** fields on the Optional Features screen are enabled.

ACD and EAS distribute calls according to the workloads and the skill levels of the agents in each hunt group. You can use this type of call distribution to track call handling and monitor the efficiency of agents. When you assign ACD to a hunt group, the group is called a split. When you assign EAS to a hunt group, the group is called a skill.

If the EAS option on the System-Parameters Customer-Options screen is active, the setting is applied to the system. Use skills for all the skills and hunt groups. After EAS is active, EAS or EAS-PHD is applicable to the hunt group, and the calls are distributed the agents.

For more information about EAS, see *Administering Avaya Aura® Call Center Elite*. For more information on about ACD and multiple call handling, see *Avaya Aura® Call Center Elite Feature Reference*.

The following table lists the different hunt group types and how each type handles incoming calls.

Group type	Hunting method	Extra software needed
circ (Circular)	The system routes calls in a round-robin order. The system directs inbound calls in the order of the administered extensions. The system tracks the last extension in the hunt group to which a call was connected. The next call to the hunt group goes to the next extension in the queue, regardless of how long that extension is idle.	None
ddc (Direct Department Calling)	Direct Department Calling (DDC) is also known as hot seat distribution. The system starts with the first extension in the hunt group and hunts for an available extension. If the first extension is busy, the system checks the second extension. If the second extension is busy, the system checks the third extension, and so on. When an extension is available or idle, the system rings that extension to connect the call. DDC provides the most equitable distribution of calls if you are not using ACD or Expert Agent Selection. DDC works with modem pools, data-line circuit ports, and data modules. DDC is unavailable if the group is administered as a skill and EAS is enabled as part of Call Center Elite administration.	None
ead-loa (Expert Agent Distribution - Least Occupied Agent)	The system hunts for the available agent who has the highest skill level and the lowest percentage of work time since the agent logged in. EAD-LOA is the most prevalent skill setting when EAS is active.	Requires EAS to be active as part of Call Center Elite administration. Business Advocate features do not have any negative impact on EAD-LOA. The system matches EAD-LOA with the Skill Level or the Greatest Need option for each agent.

Table continues…

Group type	Hunting method	Extra software needed
ead-mia (Expert Agent Distribution - Most Idle Agent)	The system hunts for the available agent who has the highest skill level and the longest idle time since the last call. 1 is the highest priority and 16 is the lowest.	Requires EAS to be active as part of Call Center Elite administration. Business Advocate features do not have any negative impact on the functioning of EAD-MIA. The system matches EAD-MIA with the Skill Level or the Greatest Need option for each agent.
pad (Percent Allocation Distribution)	The system selects an available agent, based on a comparison of work time in the skill and the target allocation for the skill.	Requires EAS and Business Advocate to be active as part of Call Center Elite administration. PAD is paired with the Percent Allocation (PA) option administered for each agent.
slm (Service Level Maximizer)	The system compares the current skill level for each administered skill with a user-defined call service level target. The system selects only those agents whose other skills require the least service of the agent at the current time. The system compares the current skill level for each administered skill with a user-defined call service level target. The service level target is answering X% calls in Y seconds. The system selects only those agents whose other skills require the least service at the current time. Therefore, under call surplus and agent surplus conditions, the arriving inbound ACD calls are distributed according to the service level targets.	Requires EAS to be active and Business Advocate to be inactive. Both SLM and Business Advocate features cannot be simultaneously active on the same Communication Manager instance. SLM is assigned to each agent and is applicable to all of the administered skills of the agents at all times, under both call surplus and agent surplus conditions.

Table continues…

Group type	Hunting method	Extra software needed
ucd-loa (Uniform Call Distribution - Least Occupied Agent)	The system hunts for the agent with the lowest percentage of work time since the agent logged in.	Requires EAS to be active as part of Call Center Elite administration. Business Advocate features do not have any negative impact on the functioning of UCD-LOA. UCD-LOA is administered according to skills and is paired with per agent option of Greatest Need as skill levels are not used.
ucd-mia (Uniform Call Distribution - Most Idle Agent)	The system hunts for the agent who is idle the longest since the last call.	None

Hunt group extension unavailability

An extension in a hunt group is unavailable to receive calls if the hunt group member is handling another call. The extension becomes unavailable if the member presses one of the following buttons:

- Hunt Group Busy, or if the member enters the Feature Access Code (FAC) for Hunt Group Busy Activate.
- Send All Calls
- Call Forwarding All Calls

Hunt Group Busy option

Hunt Group Busy position for H.323.

Hunt Group Busy Position option can be configured for H.323 in the following ways:

- FAC (Feature Access Code)
- Using Aux Work

To deactivate calls coming or terminating to extensions of a hunt group, the hunt group member must dial the Hunt Group Busy Feature Activation code followed by the hunt group number.

"To reactivate calls coming or terminating to extensions of a hunt group, the member must dial the Hunt Group Busy Deactivation code followed by the hunt group number.

Busy hunt Position feature can be activated/deactivated using AUX work button as well.

If needed, the hunt group member must add zeros before the hunt group number to ensure that the small platform hunt group has a two-digit number and the large platform hunt group has a four-digit number. For example, if a large platform uses the hunt group number 14, the hunt group member must dial the Hunt Group Busy Activation or Deactivation FAC preceded by two zeros,

therefore 0014 must be dialed. Similarly, if a small platform uses the hunt group number 2, the hunt group member must dial the Hunt Group Busy Activation or Deactivation FAC preceded by one zero, therefore 02 must be dialed.

If the last available member of a hunt group tries to activate the Hunt Group Busy option, the following events occur:

- New calls to the hunt group receive a busy tone or go to coverage.
- The system continues to route calls that are already in the queue to the last available extension.
- When the queue is empty, the system activates Hunt Group Busy. At the last available extension, if a status lamp is associated with the **Aux Work** button, the lamp flashes until the queue is empty. When no more calls remain in the queue, the system activates Hunt Group Busy and if a status lamp is provided, the lamp lights steadily, but does not flash.

If an agent is an ACD split and a hunt group member, the agent in the split usually has an **AUX work** button that also activates or deactivates the Hunt Group Busy option. If an agent is the last available member and pushes the **AUX work** button, the lamp on the button flashes until the queue is empty. The flashing light means that the agent is still available. When the queue is empty, the lamp lights but does not flash, and the system activates Hunt Group Busy.

Hunt Group Busy position for SIP

Hunt Group Busy position for SIP is similar to **Aux Work** button, except for the fact that the button is named as **hntpos-bsy** and this button can only be used for non-ACD hunt groups.

96X1 SIP endpoints supports Hunt Group Busy position feature. FAC is also available for SIP endpoints.

Send All Calls with hunt groups

If a station activates Send All Calls with the **Send All Calls** button, hunt group calls go in the queue, if a queue is administered. If a queue is not administered, callers get a busy treatment if Send All Calls is activated for all the agents.

If an extension is an agent in an ACD split and a hunt group member, the split agent usually has an **AUX-work** button that also activates and deactivates Hunt Group Busy. If an agent presses the **Send All Calls** button, the agent becomes unavailable for hunt group calls. The agent becomes available for hunt group calls again when the agent presses the **Send All Calls** button again.

Call Forwarding All Calls with hunt groups

With Call Forwarding All Calls active, an extension within a hunt group is unavailable for hunt group calls. If a forced first announcement is administered for the hunt group, callers hear the forced first announcement before the system forwards the call.

Queues for hunt groups

You can set up a queue for a hunt group. When all extensions in the group are busy, calls wait in the queue for the next available extension. You set the length of the queue to determine how many calls can wait in the queue.

If all hunt group members are unavailable or the queue is full, the system treats the call in one of the following ways:

- If the call is internal or is carried on a DID (Direct Inward Dialing), DS1 (Digital Signal Level 1), or tie trunk, the caller hears a busy tone.
- If the call is on a central office (CO) trunk, the caller hears ringing, but gets no answer.
- If the hunt group has call coverage, the system sends the call to a coverage point.

You can set up a queue warning level and an associated queue warning indicator lamp. When the queue reaches this level, the lamp lights and remains lit until the queue drops below this level. You can have one lamp for each hunt group queue. Install the lamp so that all members of the hunt group can see the lamp.

TTY hunt groups

Several laws require that “reasonable accommodation” be provided for people with disabilities. For this reason, your company might offer support for callers who use teletypewriters (TTYs).

To accommodate TTY callers, you can create a hunt group that includes agents who are equipped with a TTY. Many TTYs can connect directly to the telephone network by means of analog RJ-11 jacks. However, 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 speak clearly. These people often prefer to receive calls on the TTY, and then speak in response. The call center agent must alternate between listening on the telephone and typing on the TTY. This process is easier with an acoustically coupled configuration.

Although TTY-emulation software packages are available for personal computers, few of these software packages can mix voice and TTY on the same call.

For a TTY hunt group, you can record TTY announcements and use announcements for the hunt group queue. To record announcements for TTY, follow the same procedure that you use for voice recordings from your telephone. However, instead of speaking into your telephone to record, type the announcement with the TTY.

As an alternative to 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.

Hunt Group administration

The following tasks are part of the administration process for the Hunt Groups feature:

- Setting up hunt groups
- Changing a hunt group

- Setting up queues for hunt groups
- Adding hunt group announcements
- Administering Night Service for hunt groups

Related links

Setting up hunt groups on page 846
Changing a hunt group on page 847
Setting up queues for hunt groups on page 847
Adding hunt group announcements on page 848
Administering Night Service for hunt groups on page 848

Screens for administering Hunt Groups

Screen Name	Purpose	Fields
Announcements/Audio Sources	Record announcements for hunt groups.	As needed
Class of Service	Change the Class of Service (COS) from the default of 1.	As needed
Coverage Paths	Set up coverage paths for hunt groups.	• Ext • Type • COR • TN • Name • Others as needed
Hunt Group	Add or change hunt groups.	As needed
Call Center Optional Features	To use these call distribution methods for hunt groups, ensure that ACD and Expert Agent Selection (EAS) are set to y .	• ACD • Expert Agent Selection (EAS)
Trunk Groups	Set up night service for hunt groups.	Night Service Incoming Destination

Setting up hunt groups

Procedure

1. Enter `add hunt-group next`.

   The **Group Number** field is automatically filled in with the next available hunt group number.
2. In the **Group Name** field, type the name of the group.
3. In the **Group Extension** field, type the hunt group extension.
4. In the **Group Type** field, type the code for the call distribution method that you choose.

5. Press `Enter` to save your changes.

   The COS (Class of Service) default for all hunt groups is 1. Therefore, any changes to COS 1 on the Class of Service screen changes the COS for all hunt groups. The Hunt Group screen does not display the **COS** field.

6. Click **Next** until you see the Group Member Assignments page of the Hunt Group screen.
7. In the **Ext** field, type the extensions of the agents that you want in the hunt group.
8. Press `Enter` to save your changes.

   For more information about the other fields on the Hunt Group screen, see *Administering Avaya Aura® Communication Manager*.

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 queues for hunt groups

About this task

Use this procedure to configure Communication Manager to place hunt group calls that cannot be answered immediately in a queue.

You can also administer the system to send a warning message when the system exceeds the threshold for the number of calls in a queue and for the waiting time in a queue.

Note:

If the Expert Agent Selection (EAS) option is active along with Call Center Elite, use call vectoring commands for announcements. To simplify ongoing administration, use Dynamic Queue Slots instead of limiting queues as per skills.

For more information about administering call vectoring commands and Dynamic Queue Slots, see *Administering Avaya Aura® Call Center Elite*.

Procedure

1. On the SAT screen, enter `change hunt-group n`, where *n* is the number of the hunt group to change.
2. In the **Queue** field, type `y`.
3. In the **Queue Length** field, type the maximum number of calls that you want to wait in the queue.
4. In the **Calls Waiting Threshold** field, type the number of calls that can be in the queue before the queue status lamps flash.

5. In the **Time Warning Threshold** field, type the number of seconds for a call to wait in the queue before the queue status lamps flash.
6. Save the changes.

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.

You assign the recorded announcements to an extension. You can type `display announcements` to find the extensions of recorded announcements that are already assigned to extensions. You can use the same announcement for more than one hunt group.

For more information on recording announcements, see the Announcements feature description.

Procedure

1. Enter `change hunt-group n`, where *n* is the number of the hunt group to which you want to add the announcement.
2. In the **First Announcement Extension** field, type the extension of the announcement that you want callers to hear.
3. In the **First Announcement Delay (sec)** field, type the number of seconds that you want the caller to wait before the caller hears the first announcement.

   If you set the delay announcement interval to 0, callers automatically hear the announcement immediately. This is called a forced first announcement.
4. Press `Enter` to save your changes.

Administering 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. The destination you administer can be:

- An extension
- A recorded announcement extension
- A vector directory number (VDN)
- Another hunt group extension
- An attendant

Procedure

1. Enter `change hunt-group n`, where *n* is the number of the hunt group for which you want to administer night service.
2. In the **Night Service Destination** field, type the night service extension to which the system routs calls.

3. Select **Enter** to save your changes.
4. Program a night service button so that members of the hunt group can activate and deactivate night service. For more information on how to program feature buttons, see *Avaya Aura® Communication Manager Screen Reference*.

Considerations for Hunt Groups

This section provides information about how the Hunt Groups feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Hunt Groups feature under all conditions.

Members assigned to multiple hunt groups

An extension can be a member of more than one hunt group. However, a telephone, even a multiappearance telephone, can receive only one hunt group call at a time. On a multiappearance telephone, all appearances must be idle to receive a hunt group call.

You can assign a Coverage Incoming Call Indicator (ICI) button to a multiappearance telephone or an attendant console. When a member receives a call for the hunt group that is associated with the ICI button, the status lamp lights.

Automatic Call Distribution (ACD) agents as hunt group members

Do not include agents in an ACD split in non-ACD hunt groups if the agents also receive ACD split calls. The system distributes all ACD calls to agents in a split before the system distributes hunt group calls.

When you change an ACD split to a non-ACD hunt group, each agent in the split must dial the Hunt Group Busy deactivation code to receive calls for that hunt group. If the agent has an **AUX-work** button, the status lamp lights when you make the change. The agent can then press the button to become available for hunt group calls.

Hunt group for communications devices

Members of a hunt group that is used for shared data communications must be of the same type. Therefore, you can enter either data modules or analog modems in a hunt group, but not both. Option settings must be the same for all group members.

A caller can still use the Data Extension button to access the associated data module, even if the module is in a hunt group. Individual data modules or modems can originate and receive calls.

Access restrictions

You can use Class of Restrictions (COR) to restrict an extension from receiving calls other than those calls to the hunt group to which the extension is assigned. You can also restrict extensions on Communication Manager from calling the extension of the hunt group.

System limits

The size of your system determines how many hunt groups you can set up, and how many extensions you can assign to each group.

Trunk signaling

A hunt group always has its own extension. Therefore, a caller with a telephone on Communication Manager can dial that extension to call the hunt group. If a trunk group can pass digits from the central office (CO) to Communication Manager, for example, over a DS1 trunk group, a caller can also dial a 7-digit number. The 7-digit number consists of a specified prefix and the extension of the hunt group.

If a trunk group cannot pass digits from the CO to Communication Manager, the system can connect incoming calls to a hunt group only if the trunk group has the hunt group extension as the primary destination. This requirement includes trunk groups for incoming listed directory number (LDN) calls, international exchange calls, 800 service calls, and automatic tie-trunk calls.

Interactions for Hunt Groups

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

Attendant Call Waiting

Attendant Call Waiting does not work for calls that the attendant sends to a hunt group. Attendant Call Waiting does work for calls to individual hunt group members.

Attendant Return Call

Attendant Return Call does not work for calls that the attendant sends to a hunt group.

Automatic Callback

Automatic Callback does not work on calls to a hunt group.

Automatic Call Distribution (ACD)

ACD does not work with circular station hunting.

Call Detail Recording (CDR)

For each call, the system can record the associated hunt group extension or the member extension that answers.

Internal Automatic Answer (IAA)

Internal calls to a hunt group member are eligible for Internal Automatic Answer (IAA).

Leave Word Calling (LWC)

A hunt group can receive and store LWC messages. The following entities can retrieve LWC messages:

- One member of the hunt group
- A covering user of the group
- A system-wide message retriever

  The message retriever must have a telephone display, and proper authorization. If the message retriever is a member of the hunt group, you can assign a remote Automatic

Message Waiting lamp to the retriever. The lamp indicates when the hunt group has an LWC message.

Night Service

When the Night Service destination for a hunt group is another hunt group, callers hear the forced announcement of the first hunt group, if a forced first announcement is administered. The system then redirects the call to the night service hunt group.

Priority Calling

The system treats a priority call to a hunt group the same as a nonpriority call, except that the extension receives a distinctive three-burst ring.

Queuing

Queuing does not work with circular station hunting.

Terminating Extension Group (TEG)

A TEG cannot be a member of a hunt group.

Vectoring

Call vectoring does not work with circular station hunting.

Chapter 101: IPv6 support

Communication Manager supports dual stack. Therefore, Communication Manager can be simultaneously connected with endpoints and entities that use IPv4 and IPv6 addresses.

Communication Manager supports IPv6 solution for SIP endpoints.

Communication Manager supports the following features:

- Enhancing the support for IPv6, by introducing the Alternate Network Address Type (ANAT) mechanism to achieve media level interworking between IPv4 and IPv6.
- Supporting IPv6 address family for negotiation of media parameters with SIP entities such as SIP phones.
- Supporting IPv6 to establish connection with far-end SIP entity.
- Allowing the selection of IPv6 or IPv4 or Dual Stack media resource depending on Communication Manager configuration and far-end capabilities.

Note:

When you configure ANAT with preference IPv6 and IPv4 and configure a SIP trunk from Communication Manager 7.1.x or later to Communication Manager 7.0, then the outgoing call from Communication Manager 7.1.x or later to Communication Manager 7.0 will not work.

Note:

If you set the **Intra-region IP-IP Direct Audio** or the **Inter-region IP-IP Direct Audio** field to `n`, the outgoing call gets dropped.

Note:

When using 96xx or 96x1 (pre-7.1 firmware) deskphones with Communication Manager supporting dual stack media and using the preference IPv6/IPv4, set one of the following fields to avoid loop detection:

- Set the **Loop Detection Mode** field to `off`.
- Set the **Loop Count Threshold** field to `7`.

To set these fields on the System Manager web console, navigate to **Elements** > **Routing** > **SIP Entities**.

Enabling IPv6 addressing

About this task

The following procedure describes the settings to enable IPv6 addressing in Communication Manager.

Procedure

1. On the Communication Manager SMI page, navigate to **Server Configuration** > **Network Configuration**.
2. In the **IPv6 is Currently enable** field, select **enabled**.
3. Click **Change**.

   With this change, the system displays the IPv6 text boxes against each field.
4. Enter the IPv6 values for the default gateway, IP address, and prefix.
5. Click **Change**.
6. For the changes in the IPv6 settings to take effect, you must restart Communication Manager:
   a. In the **Server** section, click **Shutdown Server**.
   b. Ensure that the **Restart server after shutdown** field is selected and click **Shutdown**.

Enabling procr6

Procedure

1. On the Communication Manager SAT interface, type `change ip-interface procr`.
2. On page 2, in the **Enable Interface**, enter `y`.
3. Save the changes.

Configuring ANAT system wide

Procedure

1. On the Communication Manager SAT interface, type `change system-parameters ip-options`.
2. On page 3, in the **ANAT Enabled** field, type `y`.
3. Save the changes.

Configuring ANAT for each network region

Procedure

1. On the Communication Manager SAT interface, type `change ip-network region n`, where *n* is the network region number.
2. On page 2 **ANAT Enabled** field, type `y`.
3. Save the changes.

Setting address type preference in SDP

Procedure

1. On the Communication Manager SAT interface, type `change ip-codec-set n`, where *n* is the ip-codec-set number.
2. On page 2, in the **Media connection IP address type preference** field, enter one of the following:
   - `IPv4/IPv6`
   - `IPv6/IPv4`
   - `IPv4/none`
   - `Ipv6/none`

   Avaya recommends that you use IPv4/IPv6.
3. Save the changes.

Considerations for IPv6

- Specify both IPv4 and IPv6 addresses for a station on the IP Network Map screen.
- Specify both IPv4 and IPv6 addresses of LSP or ESS on the IP Network Region screen.
- Establish either the IPv4 or IPv6 entity link with Session Manager.
- Establish either the IPv4 or IPv6 entity link with Avaya Aura® Media Server.
- All Avaya Aura® core network elements should be dual stack for interoperability.
- When the Branch Session Manager IP address is configured, Communication Manager assigns Branch Session Manager IP address to the far-end signaling group.

Chapter 102: Increase in Locations and Network Regions

With the increasing need for organizations to have multiple branch offices and the need to manage bandwidth over different network regions or branches, Communication Manager now supports a maximum of 2000 locations and network regions. This increase in the number of network regions is applicable to customers who use Communication Manager installed on Dell™ PowerEdge™ R610 and HP ProLiant DL360 G7 servers.

Note:

- From Avaya Aura® Release 10.1, HP ProLiant DL360p G8 (CSR2), HP ProLiant DL360 G9 (CSR3), Dell™ PowerEdge™ R620 (CSR2), Dell™ PowerEdge™ R630 (CSR3), and Avaya Solutions Platform 120 servers are not supported.

  However, in Release 10.1, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.x, and S8300E can be upgraded to Avaya Solutions Platform S8300 R5.1.x.
- From Avaya Aura® Release 10.1, Appliance Virtualization Platform is not available for deploying or upgrading the Avaya Aura® applications. To upgrade the Avaya Aura® applications, migrate the Appliance Virtualization Platform to Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.x.

Related links

Detailed description of Network Regions on page 855
Interactions for Locations and Network Regions on page 857

Detailed description of Network Regions

Communication Manager now supports a maximum of 2000 network regions and locations. With the increase in the number of network regions, organizations can expand businesses to various locations globally. Organizations can also efficiently manage bandwidth by allocating the required amount of bandwidth to a particular network region. To support an increase of up to 2000 network regions, you can now configure network regions as core network regions and stub network regions. You can configure network regions 1 to 250 as core network regions or stub network regions. Network regions 251 to 2000 are stub network regions by default.

A core network region is the traditional network region and can have multiple direct links with other network regions. For information on core network regions, see Figure 1. Core network regions. The solid lines in the diagram indicate a direct connection between two core network regions and the dotted lines indicate an indirect logical communication path from one core network region to other core network regions. A stub network region must have a single defined pathway to only one core network region. For information on core network regions with stub network regions, see Figure 2. Core network regions with stub network regions.

Figure 1: Core network regions

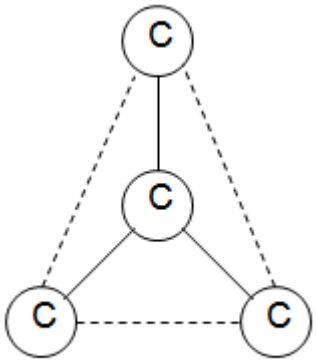
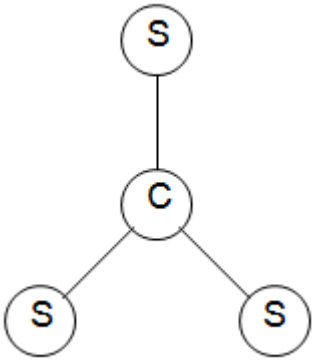
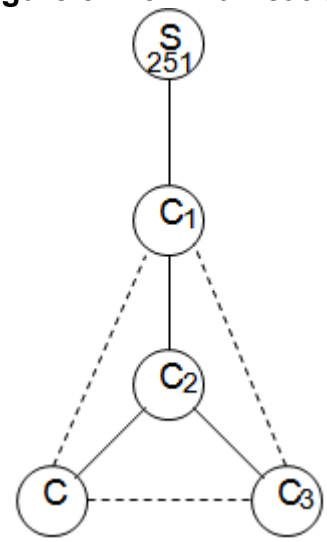


Figure 2: Core network regions with stub network regions



Stub network regions communicate with other network regions by using the defined communication pathways of the core network regions that the stub network regions are connected to. For example, if stub network region 251 is directly connected to core network region 1 and stub network region 251 needs to send data or route calls to core network region 3, then stub network region 251 first sends data to core network region 1 and from core network region 1, Communication Manager uses the predefined communication pathway of core network region 1 to reach core network region 3. For more information on communication path from stub network regions to core network regions, see Figure 3. Communication path from a stub network region to a core network region.

Figure 3: Communication path from a stub network region to a core network region



The benefit of having a stub network region is that you do not have to configure multiple communication pathways to different network regions. In previous releases of Communication Manager, when you add a network region, you must administer the communication path to all the other network regions with the associated intervening network regions. With the introduction of stub networks, when you add a stub network region, you have to administer the communication path only to the core network region that the stub network region connects to. You must assign Communication Manager hardware such as media processors, C-LANs, and cabinets to network regions 1 to 250 regardless of whether the network region is a core network region or a stub network region.

You can assign media gateways to network regions above 250.

Related links

Increase in Locations and Network Regions on page 855

Interactions for Locations and Network Regions

The increase in the number of locations and network regions can affect the following features:

Dial Plan Transparency

The Dial Plan Transparency feature can work in an endpoint-only stub network region. Stub network regions use the media processing resources of the core network regions they are connected to. If the Dial Plan Transparency feature is administered in the destination core network region of a stub network region, then during a network outage, the endpoints in the stub network region can connect to endpoints in other network regions.

Inter-gateway Alternate Routing

IGAR is not available for stub network regions from 251 to 2000, but stub network regions from 1 to 250 support IGAR if the stub network region contains a gateway or a Port Network.

Emergency Calling

Stub network regions have the location field administered in the network region forms. When an endpoint in a stub network region dials an emergency number, the ARS location table analyzes the dialed number and routes the call to the destination using a predefined route pattern.

For Communication Manager managed bandwidth, emergency calls will always connect despite administered bandwidth limit exhaustion. If the emergency calls connect despite bandwidth limit exhaustion, the **BW-Used** field under the status ip-network-region <no> page may cross the administered bandwidth limit.

Related links

Increase in Locations and Network Regions on page 855

Chapter 103: Individual Attendant Access

Using the Individual Attendant Access feature, users can call a specific attendant console. If you have more than one attendant console, you can assign an extension to each console. Users can then dial the assigned extension to call an attendant directly. With individual attendant extensions, you can allow attendants to use features that an attendant group cannot use. For example, you can assign individual attendant extensions to hunt groups.

Individual Attendant Access administration

The following task is a part of the administration process for the Individual Attendant Access feature:

- Assigning an extension to an attendant console

Related links

Assigning an extension to an attendant console on page 859

Preparing to administer Individual Attendant Access

Procedure

Set up an attendant console.

For information on how to set up an attendant console, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Individual Attendant Access

Screen name	Purpose	Fields
Attendant Console	Assign an extension to an attendant console.	Extension

Assigning an extension to an attendant console

Procedure

1. Enter `add attendant n`, where *n* is a number between 1 and 28 that you want to assign to the attendant console.
2. In the **Extension** field, type a valid extension that conforms to your dial plan.

3. Press `Enter` to save your changes.

Chapter 104: Intercom

Use the Intercom feature to administer a button that calls a predefined extension when the button is pressed. Using the Intercom feature, one user can call another user in a predefined group just by pressing a couple of buttons.

With Communication Manager R10.1.2, the auto-icom button works as follows:

- When an Intercom button is pressed that is associated with an active call, the active call is put on hold
- When an Intercom button is pressed that is associated with a call on hold, any active call is placed on hold, and the call associated with the pressed Intercom button is resumed
- When an Intercom button is pressed that is not associated with a call on the phone, an invite is sent to initiate an intercom call
- Communication Manager displays LED notifications for auto-icom feature buttons
- Communication Manager supports up to 72 Intercom buttons on each J100 type station.

Detailed description of Intercom

To control which telephones can make intercom calls to each other, you add the telephones in groups called intercom groups. Once you add a set of telephones to the group, users can make intercom calls by administering one or both of the following feature buttons on their telephones:

Automatic Intercom

Users use this button to call one predefined telephone in the same intercom group. You specify the destination extension for this button.

Dial Intercom

Users in an intercom group use this button to call anyone else in the same group. The user lifts the handset, presses the **Dial Intercom** button, and then dials a 1 digit or a 2 digit code for the extension.

Telephones with both of these capabilities can belong to the same intercom group.

Intercom groups

- You can create up to 256 intercom groups per standard and up to 1024 intercom groups with SA9035 - Increased Intercom Groups on one server that runs Communication Manager.

- Each group can contain up to 32 extensions in it.
- You can assign the same extension to different groups.
- Intercom calls are possible only between extensions in the same group.
- Any group member with a feature button for Dial Intercom can make an intercom call to any other member in the group.

Telephones in Intercom groups

- You can assign any telephone to an intercom group. However, only multi appearance telephones can make and receive intercom calls. Single-line telephones can only receive intercom calls. Multiappearance telephones must have at least one open or available call appearance to receive intercom calls.
- An intercom call makes a unique alerting sound. If the telephone has an intercom button with a status lamp, the lamp also flashes.
- You can establish an automatic intercom call between two telephones, even if the Class of Restriction (COR) does not support other calls between them.

Hold or un-hold

When there are multiple intercom calls on a station, you can press the intercom button to toggle between calls. When you press the second intercom button to answer a call, the existing call is put on hold. You can press the auto-icom button to hold or un-hold existing calls on the phone.

Intercom administration

For more information about intercom administration, see Using Telephones as Intercoms in *Administering Avaya Aura® Communication Manager*.

Interactions for Intercom

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

Bridged Appearances

Bridged appearances cannot receive Intercom calls.

Call Coverage

Unless the caller activates **Go To Cover**, intercom calls does not follow a coverage path,.

Call Forwarding

Intercom calls can be forwarded to a destination on the network or off the network.

Call Pickup and Directed Call Pickup

Call Pickup can alert and pickup intercom call if **Call Pick Alert** and **Call Pickup on Intercom Calls** are enabled. If Call Pickup on Intercom Calls is disabled, Call Pickup does not alert or allow to pickup Intercom call.

Data Privacy and Data Restriction

Extensions with either of these active features cannot originate Intercom calls.

Multi-Device Access (MDA)

Only the most recent registered device receives an intercom call landing on the extension.

Chapter 105: Internal Automatic Answer

Use the Internal Automatic Answer (IAA) feature to provide a convenient, hands-free way to answer internal calls to users who have multifunction stations with a speakerphone or a headphone.

Detailed description of Internal Automatic Answer

With the Internal Automatic Answer (IAA) feature, the called telephone can accept a call and answer the call automatically. The called telephone cannot accept a call if the telephone is in the process of dialing digits or has a call on hold.

When the user presses the IAA feature button, the system turns on the status lamp and activates the feature. When the user presses the same button again, the system deactivates the feature and turns off the status lamp. Pressing the feature button has no effect on an active call or a ringing call. Using the speakerphone to place calls does not affect the state of IAA.

When an IAA-enabled phone answers a call, the calling telephone does not receive the ringback tone. The called telephone receives a ring ping followed by the Incoming Caller ID tone, which sounds like tweedle-dee. Communication Manager turns on the speaker and the microphone of the called telephone. The called telephone then connects to the calling party.

Note:

While the system plays the Incoming Caller ID tone, the called party can hear the tone and the calling party. However, the calling party does not hear any tone and hears the called party only after the Incoming Caller ID tone is completed.

If a user has an active IAA and is currently busy on a call, or in the process of dialing digits, subsequent incoming calls are treated as if IAA is inactive.

The following internal calls are eligible for IAA:

- Station-to-station voice calls, with both telephones on the same server. These calls include redirected intraswitch calls. To use IAA for these calls, you must set the **Internal Auto-Answer of Attd-Extended/Transferred Calls** field on the Feature-Related System Parameters screen to transferred or both.
- Internal call from another node in a Distributed Communications System (DCS) configuration. These calls are from an internal, non attendant telephone on that node and includes redirected inter-DCS calls. To use IAA for these calls, you must set the **Internal**

Auto-Answer of Attd-Extended/Transferred Calls field on the Feature-Related System Parameters screen to transferred or both.

- Attendant-extended external calls. You must set the **Internal Auto-Answer of Attd-Extended/Transferred Calls** field on the Feature-Related System Parameters screen to attd-extended or both.

The following calls are ineligible for IAA:

- Calls from public network trunks, including Private Central Office Line (PCOL)
- Calls from non-DCS tie trunks
- Automatic Callback calls
- Automatic Circuit Assurance calls
- Data calls
- Attendant-extended external calls if you set the **Internal Auto-Answer for Attd Extended/ Transferred Calls** field on the Feature-Related System Parameters screen to transferred or none.
- Calls that the system redirects because of an overflow of Emergency Access to the Attendant calls in the queue.
- Calls when you set the **Active Station Ringing** field of the receiving telephone on the Feature-Related System Parameters screen to continuous.

Administering Internal Automatic Answer

This section describes the screens that you use to administer the Internal Automatic Answer (IAA) feature.

Screens for administering Internal Automatic Answer

Screen name	Purpose	Fields
Feature-Related System Parameters	Set up IAA at a system level.	Internal Auto-Answer of Attd-Extended/ Transferred Calls

Considerations for Internal Automatic Answer

This section provides information about how the Internal Automatic Answer (IAA) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits

of Internal Automatic Answer under all conditions. The following considerations apply to Internal Automatic Answer:

- Users must always deactivate IAA when the users leave the work area. If users do not deactivate IAA, the unattended station might unintentionally answer incoming calls, instead of sending all the calls.
- A 602A terminal is off-hook when the headset or the speakerphone is connected. Therefore, IAA answers a call if all other call appearances are idle.

Interactions for Internal Automatic Answer

This section provides information about how the Internal Automatic Answer (IAA) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Internal Automatic Answer in any feature configuration.

Attendant Console

IAA is unavailable with Attendant Console.

Automatic Answer

You cannot administer both IAA and Automatic Answer simultaneously on the same telephone.

Automatic Call Distribution (ACD)

Calls that are directed to an ACD split are eligible for IAA.

Automatic Callback

Callback calls by way of Automatic Callback are unanswered automatically by IAA.

Automatic Circuit Assurance (ACA)

Calls that are generated by ACA are ineligible for IAA.

Bridged Call Appearance - Multiappearance Telephone

Calls that terminate on a bridged call appearance are ineligible for IAA at the bridged station, even if the bridged station has IAA active. However, IAA can be used by the principal station to answer the call.

Bridged Call Appearance - Single-Line Telephone

Calls that terminate to a bridged call appearance are ineligible for IAA at the bridged station, even if the bridged station has IAA active.

Call Coverage

If an internal call is redirected to another telephone by Call Coverage redirection criteria, that call is eligible for IAA at the redirected telephone.

IAA does not apply to calls to the original called extension when:

- The called telephone has Send All Calls active.
- The calling telephone selects Go to Cover before placing the call

Calls that are directed to a coverage answering group are ineligible for IAA.

Note:

If you set the coverage path for a telephone to All Calls, and that telephone activates IAA, the first coverage point hears a ring. Then the principal station automatically answers, and the coverage-simulated bridge is dropped. The coverage station rings, but is unable to answer the call, because the coverage-simulated bridge was dropped.

Call Forwarding

Calls to a telephone with IAA and Call Forwarding active are forwarded, and are unanswered by the station dialed.

Note:

If the forwarded-to telephone is internal and has IAA active, the forwarded-to telephone automatically answers the redirected call.

Call Park

If you are using Deluxe Paging and Call Park times out, the call returns to the originating telephone that parked the call, and is eligible for IAA.

Call Pickup

IAA can answer internal calls to a telephone in a Call Pickup group. If the called extension in a Call Pickup group has IAA-active, the call is automatically answered. A telephone with an active IAA cannot automatically answer calls to other telephones in its Call Pickup group.

Conference

IAA can answer internal conference calls. If more than one party has joins a conference call through automatic answer, the parties remain connected until the parties disconnect, or the controlling party drops the call.

Data Call Setup

Data calls are ineligible for IAA.

Direct Department Calling (DDC) and Uniform Call Distribution (UCD)

Internal calls to a member of a DDC or a member of a UCD group member are eligible for IAA.

Distributed Communications System (DCS)

If a call is from an internal telephone on another server or switch in a DCS configuration, that call is considered internal and is eligible for automatic answer.

Do Not Disturb

Do Not Disturb preempts IAA at the called telephone.

Go to Cover

IAA does not apply to calls to the original called extension when the calling telephone selects Go to Cover before placing a call.

ISDN-BRI

IAA is unavailable with ISDN-BRI telephones.

Loudspeaker Paging - Deluxe Paging

If Call Park times out when you are using Deluxe Paging, the call returns to the originating telephone that parked the call. Such calls are eligible for IAA.

Ringback Queuing

Automatic calls that are generated by Ringback Queuing are ineligible for IAA.

Send All Calls

IAA does not apply to calls to extensions with Send All Calls is active.

Terminating Extension Group (TEG)

Calls to a TEG extension are ineligible for IAA. However, calls to an individual extension are eligible.

Chapter 106: Inter-Gateway Alternate Routing for SIP endpoints

With the Inter-Gateway Alternate Routing (IGAR) feature, Communication Manager can use the PSTN when the IP-WAN cannot carry the bearer connection for the single-server systems that use the IP-WAN to connect bearer traffic between port networks or gateways.

Note:

Communication Manager Release 6.3.5 and earlier supported IGAR for analog, DCP, and H.323 endpoints. Communication Manager Release 6.3.6 or later extends this support to SIP endpoints.

Related links

Detailed description of IGAR on page 869
Administering IGAR on page 871
Configuring IGAR parameters for the network region on page 871
Displaying the number of IGAR connections on page 872
Viewing the status of IGAR on a trunk on page 872
Interactions for IGAR on page 872

Detailed description of IGAR

IGAR requests PSTN to provide bearer connections in any of the following conditions:

- The number of calls allocated or bandwidth allocated through Call Admission Control-Bandwidth Limits (CAC-BL) is reached.
- VoIP RTP resource exhaustion in a port network or media gateway is encountered.
- The codec set between a pair of network regions is set to `pstn`.
- Forced redirection is configured between a pair of network regions.

IGAR provides enhanced Quality of Service (QoS) to large distributed single-server configurations. You can use IGAR for configurations where the IP network is not reliable enough to carry bearer traffic. If you have more than one IP network available, you can use H.323 or SIP trunks for IGAR instead of the PSTN.

When Communication Manager needs an inter gateway connection and adequate IP bandwidth is unavailable, Communication Manager attempts to substitute a trunk connection for the IP connection. For example, Communication Manager can substitute a trunk connection in any of the following situations:

- A user in one Network Region (NR) calls a user in another NR.
- A station in one NR bridges on to a call appearance of a station in another NR.
- An incoming trunk in one NR routes to a hunt group with agents in another NR.
- An announcement or music source from one NR must be played to a party in another NR.

Communication Manager attempts to use a trunk for inter-region voice bearer connection when the following five conditions are met:

- An inter gateway connection is needed.
- IGAR requests PSTN to provide bearer connections.
- IGAR is enabled for the NRs associated with each end of the call.
- The **Enable Inter-Gateway Alternate Routing** system parameter is set to `y`.
- The number of trunks used by IGAR in each NR has not reached the limit administered for that NR.

The SRC PORT TO DEST PORT TALKPATH page of the status station screen shows the IGAR trunk connectivity for an interNR call.

A Trunk Inter-Gateway Connection (IGC) is established using ARS to route a trunk call from one NR to IGAR Listed Directory Number (LDN) extension administered for the other NR. The Trunk IGC is independent of the call being placed. Therefore, Communication Manager can originate the IGC from the NR of the calling party to the NR of the called party, or vice versa. However, for users who use Facility Restriction Levels or Toll Restriction to determine who gets access to IGAR resources during a WAN outage, the calling user is considered the originator of the Trunk IGC for authorization and routing. However, if the outgoing trunk group is administered to send the Calling Number, the IGAR Extension in the originating NR is used to create this number using the appropriate administration.

The following are examples of failure scenarios and how Communication Manager handles the scenarios:

- On a direct call, the call continues to the first coverage point of the unreachable called endpoint, or if no coverage path is assigned, busy tone is played to the calling party.
- If the unreachable endpoint is being accessed through a coverage path, the coverage point is skipped.
- If the unreachable endpoint is the next available agent in a hunt group, that agent is considered unavailable, and the system tries to route the call to another agent using the administered group type, such as Circular distribution and Percent Allocation Distribution.

Related links

Inter-Gateway Alternate Routing for SIP endpoints on page 869

Administering IGAR

Procedure

1. Type `change system-parameters features`.
2. In the **Enable Inter-Gateway Alternate Routing** field, type `y`.
3. In the **IGAR over IP trunks** field, type:
   - `allow` to use H.323 or SIP trunks when selecting a trunk from a Route Pattern.
   - `skip` to skip H.323 or SIP trunks when selecting a trunk from a Route Pattern.
4. Save the changes.

Related links

Inter-Gateway Alternate Routing for SIP endpoints on page 869

Configuring IGAR parameters for the network region

Procedure

1. Type `change ip-network-region` *n*, where *n* is the network region number.
2. Press `Enter`.

   The system displays the IP NETWORK REGION screen.
3. On page 3, in the **Incoming LDN Extension** field, type an unassigned extension.
4. In the **Conversion To Full Public Number-Delete** field, type the number of digits to delete.
5. In the **Insert** field, type the digits that must be inserted before the extension to convert the number that Communication Manager can route through ARS.
6. In the **Maximum Number of Trunks to Use** field, type a value to limit the number of trunks.
7. On page 4, for a network region pair, in the **IGAR** field, type:
   - `y` to enable IGAR.
   - `n` to disable IGAR.
   - `f` to force all bearer traffic across PSTN.
8. In the **WAN-BW-limits Units** and **WAN-BW-limits Total** fields, specify the bandwidth limits.

Related links

Inter-Gateway Alternate Routing for SIP endpoints on page 869

Displaying the number of IGAR connections

Procedure

1. Type `status ip-network-region n`, where *n* is the network region number.
2. The **IGAR Now/Today** field displays the following information:
   - The number of active IGAR connections for a pair of network regions.
   - The number of times IGAR is invoked for a pair of network regions since the previous midnight.
3. The **BW-Used(bits)** field displays the bandwidth use for each call.

Related links

Inter-Gateway Alternate Routing for SIP endpoints on page 869

Viewing the status of IGAR on a trunk

Procedure

1. Type `status trunk n`, where *n* is the trunk group number.
2. On the Trunk group status screen, the **IGAR connection** field displays the status of IGAR on the trunk.

Related links

Inter-Gateway Alternate Routing for SIP endpoints on page 869

Interactions for IGAR

Attendant

If a call made directly to or redirected to the attendant group is routed to an attendant through IGAR, that attendant will not be alerted until the trunk is active.

Alternate Facility Restriction Levels

If a user has administered the alternate FRL, IGAR uses this FRL instead of the default FRL for selecting a trunk.

Call Redirection

IGAR routes the call to the destination by using the alternate route specified regardless of the redirection feature active on the extension. After the call reaches the destination using IGAR, normal call redirection occurs.

Meet-Me Conferencing

If the first Meet-Me vector step is not an announcement, but IGAR is triggered for the call, the caller hears silence for a few seconds until the Trunk IGC is active.

Station Locking

Communication Manager routes the outgoing trunk IGC by using the COR of the station that made the initial call. Therefore, a locked station whose Station Lock COR blocks the outgoing trunk calls cannot use IGAR. The station can use IGAR only when the station is unlocked.

Announcement

When IGAR is required to connect a nonrepeating announcement to a party, Communication Manager waits until the trunk IGC is active before playing the announcement.

Auto answer

When IGAR is required on a call to a party with Auto answer enabled, Communication Manager waits until the trunk IGC is active before initiating the autoanswer.

Hunt Group

If a call made to a hunt group is routed to an agent through IGAR, the agent is not alerted until the trunk IGC is active.

Malicious Call Trace (MCT)

If an agent or any station activates MCT for a call that is routed through a trunk IGC, the trunk does not appear in the MCT display or history.

However, if an incoming malicious call is connected to the called party through a trunk IGC, the system displays the incoming trunk in the MCT display and history.

Automatic Wakeup

If an announcement is administered for automatic wakeup calls, IGAR might be used to connect the announcement to the hotel guest telephone.

Call Detail Recording (CDR)

CDR records are created for IGAR calls.

Emergency Calls (E911)

If a station dials an emergency number, and the only available outgoing trunk is in a Network Region accessible only by IGAR, the calling party information is sent over the outgoing trunk while the IGAR connection is set up. Thus, even if the IGAR connection fails, emergency responders are notified of the emergency call.

Personal Central Office Line (PCOL)

If the PCOL button on a voice terminal is associated with a trunk in a different Network Region, IGAR might be required to set up the connection. The user hears the local dial tone, and any digits dialed are buffered and sent when the IGAR trunk becomes active.

Automatic Alternate Routing (AAR)

Although Communication Manager selects a trunk for IGAR by using ARS, the users can use ARS Digit Conversion to convert the number to a private-network number and use AAR instead.

Tenant Partitioning

Tenant Partitioning can block a tenant from calling another tenant and from using trunks allocated to another tenant. If IGAR is triggered on a call between tenants, IGAR can use trunks assigned to either tenant to set up the Trunk IGC.

Trunk-to-Trunk Transfer

The Trunk-to-Trunk Transfer system parameter does not control whether a call that includes a Trunk IGC can be transferred.

Trunk Access Code (TAC) Dialing

When a user dials the TAC of a trunk group in a different Network Region, IGAR might be required to set up the connection. In most cases, the user hears the local dial tone, and any digits dialed are buffered and sent when the IGAR trunk becomes active.

Stub and Core Network Region

If a stub NR numbered in the range 1-250 has a media gateway or port network, IGAR can be used directly to and from one of these stub NRs.

The NRs from 251-2000 are all stub NRs and cannot have a media gateway or port network. IGAR might be part of the end-to-end media path for endpoints in the stub NR if the associated core NR has a media gateway or port network. However, IGAR cannot be used from the stub NR (251-2000) to the core NR.

Group Paging

If an endpoint in the paging group requires IGAR for the connection, the endpoint might not hear the first few seconds of the page.

Transfer

When a call using an IGAR trunk is transferred and the transferred call no longer needs the IGAR trunk, the IGAR trunk is dropped after the new nontrunk connection is ready.

Call Pickup

if IGAR is triggered and a user picks up the call quickly, the user hears silence for a few seconds until the Trunk IGC is active.

Trunk Answer Any Station (TAAS)

If IGAR is triggered because the incoming trunk is in another Network Region from the TAAS External Alert port, and a user enables TAAS quickly, the user hears silence for a few seconds until the Trunk IGC is active.

Bridging

When a user with a bridged call appearance button presses that button and a Trunk IGC is needed to connect the user to the call, the user notices a delay before hearing the ongoing conversation.

Call Coverage Redirected Off-Net (CCRON)

CCRON involves outgoing trunk calls. Therefore, CCRON works even if there is a delay in the voice path between the calling station and the trunk to the remote coverage party.

Coverage Answer Group

If IGAR is triggered on a call that is redirected to a Coverage Answer Group, a single Trunk IGC is created between the calling party and every Network Region of the group.

Call Waiting

The Call Waiting tone for an incoming call is not played to an analog user on the existing call until the trunk requested by IGAR is active.

Terminating Extension Group

If IGAR is triggered on a call that is redirected to a Terminating Extension Group, a single Trunk IGC is created between the calling party and every Network Region of the group.

Display Charge Advice or PPM

The charging information or PPM received from the PSTN for a trunk used by IGAR is not displayed. However, the information is recorded in CDR.

Initial IP-IP Direct Media

For an incoming call from a trunk that has Initial IP-IP Direct Media enabled and if the call routes to another SIP trunk, the IGAR is set up only after the call is answered by the terminating party. Due to this setting, there might be a delay of about 5-10 seconds for talkpath setup.

Multi-Level Precedence and Preemption (MLPP)

In a Defense Switched Network (DSN), IGAR treats an MLPP call in the same manner as any other call.

Video calls

If a new video call has insufficient video bandwidth but has sufficient bandwidth for an audio call, the call continues without the video component. However, if the bandwidth is insufficient for both video and audio, the call can trigger IGAR and get a trunk IGC. The trunk IGC is used only for the audio media.

Multi-Device Access (MDA)

If a user has registered several SIP endpoints by using MDA, and not all endpoints are in the same NR, the NR of the endpoint that the user uses to make and receive calls determines whether Communication Manager creates a trunk IGC for a call.

Dual Registration

If a user has registered both an H.323 and a SIP endpoint by using Dual Registration, Communication Manager stores the NR of:

- The H.323 endpoint only once when the endpoint registers.
- The SIP endpoint every time the SIP endpoint makes or receives a call.

If the user becomes active at the H.323 endpoint after making calls through the SIP endpoint, Communication Manager triggers IGAR and sets up the trunk IGC to the SIP location.

Related links

Inter-Gateway Alternate Routing for SIP endpoints on page 869

Chapter 107: Inter-PBX Attendant Service

Attendants who support multiple location can use the Inter-PBX Attendant Service (IAS) feature to work at a single location.

Detailed description of Inter-PBX Attendant Service

With IAS, attendants can work at one location while the attendants support users at other locations. The system routes any incoming trunk calls that are to a user location, and any attendant-seeking calls, over tie trunks to the attendant location.

Inter-PBX Attendant Service administration

This section contains prerequisites and the screens for administering the Inter-PBX Attendant Service (IAS) feature.

The following task is part of the administration process for the Inter-PBX Attendant Service feature:

- Enabling Inter-PBX Attendant Service

Related links

Enabling Inter-PBX Attendant Service on page 877

Preparing to administer Inter-PBX Attendant Service

Procedure

1. Set up an attendant console.

   For information on how to set up an attendant console, see the *Administering Avaya Aura® Communication Manager*.

2. View the Optional Features screen, and ensure that the **Centralized Attendant** field is set to n.

   If you have set the **Centralized Attendant** field to y, your system does not support the Inter-PBX Attendant Service feature. Go to the Avaya Support website at

http://support.avaya.com for current documentation and knowledge articles related to administering Inter-PBX Attendant Service, or to open a service request.

Enter `display system-parameters customer-options`.

Screens for administering Inter-PBX Attendant Service

Screen name	Purpose	Fields
Console Parameters	Enable IAS.	• IAS Att. Access Code • IAS (Branch)? • IAS Tie Trunk Group No.

Enabling Inter-PBX Attendant Service

Procedure

1. Enter `change console-parameters`.
2. In the **IAS Att.Access Code** field, type the extension of the attendant group at the main server that runs Communication Manager.

   Note:

   You must type `y` in this field if the **IAS (Branch)** field is set to y.

   The system displays the **IAS Att. Access Code** field only if the **Centralized Attendant** field on the Optional Features screen is set to n.
3. In the **IAS (Branch)** field, type `y`.

   The system displays this field only if the **Centralized Attendant** field on the Optional Features screen is set to n.
4. In the **IAS Tie Trunk Group No.** field, type the number of the tie trunk group to the main IAS location. For the valid entries that you can use in this field, see *Avaya Aura® Communication Manager System Capacities Table*.

   Note:

   You must complete this field if the **IAS (Branch)** field is set to y.

   The system displays this field only if the **Centralized Attendant** field on the Optional Features screen is set to n.
5. Press `Enter` to save your changes.

Interactions for Inter-PBX Attendant Service

This section provides information about how the Inter-PBX Attendant Service (IAS) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Inter-PBX Attendant Service in any feature configuration.

Centralized Attendant Service

IAS does not work with Centralized Attendant Service

Chapter 108: 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.

Detailed description of IP DECT

The IP DECT system provides a complete integration of voice functions. The communication is done through IP trunks using the H.323/X-mobile interface. The IP DECT stations on Communication Manager side uses the XMOBILE station type.

The IP DECT R4 system includes the DECT R4 IP Base Station and the 3720 and 3725 DECT handsets. There is one IP Base Station Master, one IP Base Station Standby Master and the DECT Radio Based Stations, all of which reside on the IP network. The Avaya In-Building Wireless Server (AIWS) provides additional capabilities, such as messaging, centralized phonebook, device administration over the air to the IP DECT R4 system and can be integrated with external applications, such as different alarm systems through OAP interface.

The legacy IP DECT system includes the Avaya DECT Mobility Manager (ADMM) and DECT Radio Based Stations, all of which reside on the IP network, and Avaya 3701 and 3711 IP DECT handsets.

Upgrade scenarios

The following occurs after a Communication Manager upgrade:

- If the Multi-Location Call Routing for IP DECT feature was enabled on the Special Applications screen, the value of the **Location for Routing Incoming Calls** (previously known as **Location Routing InC Calls**) field for signaling groups of type H.323 is retained.
- If the PHS X-Station Mobility over IP DECT feature was enabled on the Special Applications screen,
  - Signaling groups of type H.323 with an **X-Mobility/Wireless Type** of DECT is retained.
  - If the X-MOBILE station (**XMOBILE Type** field is DECT) has an associated **Mobility Trunk Group** field which uses an ISDN-PRI signaling group, the value of the **XMOBILE Type** field is retained.

- If the X-MOBILE station (**XMOBILE Type** field is DECT) has an associated **Mobility Trunk Group** field which uses an H.323 signaling group, the value of the **XMOBILE Type** field is changed to IPDECT.

IP DECT administration

The following tasks are part of the administration process for the IP DECT feature:

- Enabling multiple locations for IP DECT
- Verifying system capacities
- Assigning the codec for IP DECT
- Configuring the codec used for the selected network region
- Configuring the trunk group
- Configuring the signaling group
- Configuring the station

For information on how to administer the above tasks, see *Administering Avaya Aura® Communication Manager*.

For more information on how to install and administer the IP DECT system, see *Avaya DECT R4, Installation and Administration Manual*, 21-603363.

Screens for administering IP DECT

Screen name	Purpose	Fields
Optional Features	Ensure that Multiple Locations is enabled if required.	Multiple Locations
System Capacity	Ensure that the system displays the current number of IP DECT stations.	XMOBILE Stations ISDN DECT IP DECT
IP Codec Set	Assign the codec for IP DECT configurations.	Audio Codec Silence Suppression Frame Per Pkt Media Encryption
IP Network Region	Administer the network region for IP DECT.	Codec Set RSVP Enabled Inter Network Region table

Table continues…

Screen name	Purpose	Fields
Trunk Group	Administer the trunk groups for IP DECT.	Group Type Direction Carrier Medium Service Type Codeset to Send Display Supplementary Service Protocol Digit Handling (in/out) NCA-TSC Trunk Member Send Name Send Calling Number Send Connected Number
Signaling Group	Administer the signaling groups for IP DECT.	Group Type Max number of NCA TSC Max number of CA TSC Trunk Group for NCA TSC Trunk Group for Channel Selection TSC Supplementary Service Protocol X-Mobility/Wireless Type Location for Routing Incoming Calls Near-end /Far-end Listen Ports Far-end Network Region Calls Share IP Signaling Connection Interworking Message Enable Layer 3 Test
Station	Administer the stations for IP DECT.	Type XMOBILE Type Message Lamp Ext Display Module Message Waiting Type Length of Display Mobility Trunk Group Mapping Mode

Interactions for IP DECT

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

Abbreviated Dialing

The IP DECT station uses the Abbreviated Dialing List feature access codes to dial the station, group and system abbreviated dial lists (as administered per station).

Analog – Generic

The IP DECT station can be treated as an analog station in terms of feature interactions.

Analog Disconnect

Communication Manager supports the Analog Disconnect with dial tone after 10 seconds feature for IP DECT.

Announcement

The IP DECT station initiates the Announcement feature to record an announcement by dialing the Announcement feature access code.

Attendant

The IP DECT station reaches an Attendant by dialing the Attendant feature access code.

Automatic Alternate Routing

The IP DECT station initiates an Automatic Alternate Routing (AAR) call by dialing the AAR feature access code.

Automatic Call Back

The IP DECT station initiates or receives an Automatic Call Back (ACB) call by dialing the ACB feature access code.

Automatic Call Distribution

The IP DECT station uses the various Automatic Call Distribution (ACD) features. The ACD features can be activated by dialing the following ACD feature access codes:

- After Call Work
- Assist
- Auto-In
- Aux Work
- Login
- Logout
- Manual-in
- Service Observing Listen Only
- Service Observing Listen/Talk

- Service Observing No Talk
- Add Agent Skill
- Remove Agent Skill
- Remote Logout of Agent

These features do not provide ACD-related display update to the IP DECT telephones. If the IP DECT telephone is out of a coverage area, is turned off, or has a low battery, Communication Manager has no knowledge in these scenarios. As a result, Communication Manager cannot accept service from the IP DECT telephones.

Automatic Route Selection

The IP DECT station initiates an Automatic Route Selection (ARS) call by dialing the ARS feature access code.

Bridged appearance

The IP DECT station can be an analog-bridged appearance on another station, or can be administered as a bridged appearance (analog or regular) of a station.

The bridge appearance status LEDs reflects the status of the IP DECT station. The IP DECT station can bridge calls as in any other bridge of a directly connected wired station. The MWI of the station can be set to the principal extension or the bridged extension.

Note:

If IP DECT station is a bridged appearance of a station and already in a call, no call waiting tone is sent to the handset and no display update is visible for the second incoming call.

Call Admission Control

The IP DECT configuration supports Call Admission Control bandwidth limits between any pair of IP network regions.

Call Coverage

When coverage is administered for the IP DECT station, if the station (Ring No Answer, Subscriber Absent, or Busy) does not answer the call, the X-mobile station sends calls to coverage. The IP DECT station can be a coverage point and supports the IP DECT reject feature.

If the IP DECT station is out of system, silent charging, or the user presses the reject button, IP DECT system drops the alerting call. If the station has no answer coverage, the call immediately goes to coverage. If the station is a coverage point, the call immediately progress to the next coverage point. In both the cases, the call does not drop and the caller continues to receive ringback.

If the IP DECT station is a bridge, the reject button will have the above affect. The coverage path used is that of the principal, not the IP DECT station.

Call forwarding

The IP DECT station can activate and deactivate all options for call forwarding, extended call forwarding, and enhanced call forwarding using the various call forwarding feature access codes. The remote station state can be used to determine if call forwarding criteria is met. If the remote station is busy, the criteria is met. If the remote station does not answer the call, Ring No Answer criteria is met. The IP DECT can be the station that is call forwarded to and supports the IP DECT reject feature.

If the IP DECT is out of system, silent charging, or the user presses the reject button, IP DECT system drops the alerting call. If the station has no answer forwarding, the call immediately forwards. Coverage after forwarding may still take place. In both the cases, the call does not drop and the caller can continue to receive ringback.

If the IP DECT station is a bridge, the reject button will have the above effect. The forwarding used is that of the principal, not the IP DECT station.

Call Park or Answer Back

The IP DECT station can park its current call after a flash operation by using the Call Park feature access code. The IP DECT station can answer a parked call by using the Answer Back feature access code.

Call Pickup

The IP DECT station can be in a Call Pickup Group and use the Call Pickup, Directed Call Pickup, Directed Group Call Pickup, and Extended Group Call Pickup feature access codes.

Pickup groups containing IP DECT can be in the Extended Groups. As a result, IP DECT handsets can pickup calls from other pickup groups in the same way the analog-wired stations can.

Call Shuttle

If the IP DECT feature is administered as a call shuttle, the station is alerted through call waiting tone when another incoming call arrives for it while the IP DECT station is on a call. The IP DECT station can accept the second call automatically through a flash operation. This puts the first party on soft hold. Subsequent flash operations shuttle between the second and first parties result in clearing the current call and recalling the IP DECT station to attempt to reconnect the soft held party.

Call Vectoring

The IP DECT station can change the values of variables used in the Call Vectoring feature. The values can be changed by dialing the following Call Vectoring or Prompting feature access codes:

- Converse Data Return Code
- Vector Variables 1-9

Call Waiting

When a call arrives for the IP DECT station and Call Waiting is administered, Call Waiting Tone is applied as defined by the operations of Communication Manager.

CAS Remote Hold or Answer Hold-Unhold

The IP DECT station uses the CAS Remote Hold or Answer Hold-Unhold feature access code to put a call on hard hold and to retrieve a call from hard hold.

CDR Account Code

The IP DECT station enters a CDR Account Code by dialing the CDR Account Code feature access code.

Change COR

The IP DECT station can change its COR by dialing the Change COR feature access code.

Change Coverage

The IP DECT station can change its coverage path by dialing the Change Coverage feature access code.

Codec selection

Communication Manager use the codecs administered on the IP Codec Set screen corresponding to the IP Network Region for the H.323 signaling group pointing to IP DECT system and negotiate the codecs to use with IP DECT system as in H.323.

Conference

The flash operation is sent by pressing the R-Key on the IP DECT handset. If the IP DECT initiates a second call by a previous flash operation and the third party answer the second call, then a flash operation conference all three parties. If the IP DECT initiates another flash operation, the IP DECT drops the last added party. If the IP DECT telephone drops from the conference and hence is now idle, the remaining parties on the conference call stay connected.

To activate a conference you need to enable the **Allow Conference via Flash** field on the Feature-Related System Parameters screen, otherwise the flash operation (R-key) puts the active call on hold and brings up the held call to active state.

Connection Failover with Master Base Station

Upon a connection failover during an ongoing IP DECT to IP DECT call, the secondary base station takes over. However the very first call made from either of the IP DECT extension shall not succeed. From then on, any further call from either of the IP DECT will be successful.

Connection Preservation for Branch Gateways Failover and Failback

Connection preservation for Branch Gateways in Failover and Failback does not support H.323 trunks. As a result, this feature does not work for IP DECT configurations.

Contact Closure

The IP DECT station performs various Contact Closure features by dialing the Contact Closure feature access codes.

Coverage Answer Group

The IP DECT station can be a member of a coverage answer group (as a primary appearance only).

EC500

The IP DECT can change a cell phone number associated with the EC500 feature by dialing the EC500 Self Administration feature access code.

The IP DECT can activate or deactivate the enhanced EC500 feature by dialing the EC500 Self Administration feature access code.

Emergency Calling

The IP DECT can reach the attendant in an emergency by dialing the Emergency Access to Attendant feature access code.

Extended numbering plan

The IP DECT station supports an extended numbering plan.

Facility restriction

The IP DECT system is marked with a specific Class of Restriction (COR) and Class of Service (COS), which affect toll calling and general calling permissions and restrictions.

Facility test call

The IP DECT system initiates a facility test call for a testing a trunk by dialing the Facility Test Call feature access code.

Flash Access Code

The IP DECT system sends a flash signal to the central office switch by dialing the Flash feature access code.

Group Control Restrict

The IP DECT system changes the restriction levels for all users within a given class of restriction by dialing the Group Control Restrict Activation or Deactivation feature access codes. To do this, you must have console permissions assigned to your Class of Service (COS) for the station.

Hold and Enquiry Call

The IP DECT system places an existing call on hold and makes a new enquiry call using the flash hook operation. The Hold feature behaves in a similar manner as an analog telephone. When the enquiry call is over or has not reached successfully, the IP DECT can return to the original call. Music-on-hold applies, when administered, to the held station.

Hospitality features

The IP DECT system uses the various Hospitality features. You must enable the Hospitality features for the following Hospitality feature access codes to work:

- Automatic Wakeup Call
- Housekeeping Status (Client Room)
- Housekeeping Status (Station)
- Verify Wakeup Announcement
- Voice Do Not Disturb

Hunting

The IP DECT station can be a member of a hunt group (as a primary, not a bridge). When the WT is turned off or out of range, the WT is treated as busy and Communication Manager will hunt to the next member.

The IP DECT station makes itself busy or available for hunt group functionality by dialing the Hunt Group Busy Activation or Deactivation feature access codes.

The IP DECT station can be a part of a station hunting chain as administered through the **Hunt-to-Station** field on the Station screen.

Inter-Gateway Alternate Routing

IP DECT system configurations supports Inter-Gateway Alternate Routing (IGAR) configurations.

ISDN call

The IP DECT station places an ISDN call without using ARS, AAR or UDP by dialing the ISDN feature access code.

Last Number Dialed

The IP DECT station can redial the last number dialed by the station by dialing the Last Number Dialed feature access code.

Malicious Call Trace

The IP DECT station can start and stop a Malicious Call Trace by dialing the Malicious Call Trace Activation or Deactivation feature access codes.

Meet-me Conference

The IP DECT station can dial into a Meet-me Conference.

The IP DECT station can change the Meet-me Conference access code by dialing the Meet-me Conference Access Code Change feature access code.

Multiple Precedence and Preemption

The IP DECT system uses the various Multiple Precedence and Preemption (MLPP) features. You must enable the MLPP features for the following MLPP feature access codes to work:

- Precedence Calling
- Worldwide Number and Dial Plan Precedence Access Codes for
  - Flash override preemption level
  - Flash preemption level
  - Immediate preemption level
  - Priority preemption level
  - Routine preemption level

Per Call CPN

The IP DECT system blocks or unblocks CPN on a trunk call by dialing the Per Call CPN Blocking or Unblocking Code feature access codes.

PIN Checking

The IP DECT system invokes the PIN Checking feature by dialing the following feature access codes:

- PIN Checking for Private Calls
- PIN Checking for Private Calls Using ARS
- PIN Checking for Private Calls Using AAR

Posted Messages

The IP DECT system invokes or cancels a posted message by dialing the Posted Messages Activation or Deactivation feature access codes.

Priority Calling

The IP DECT system initiates a priority call by dialing the Priority Calling feature access code.

Program AD lists

The IP DECT system initiates the Program AD List feature by dialing the Program feature access code.

The IP DECT system initiates the Abbreviated Dial Program Group List feature by dialing the Abbreviated Dial-Program Group List feature access code, if they have permission to do so.

Reset Shift Dial

The IP DECT system can use reset shift dialing for user controlled call redirection.

Send All Calls

The IP DECT system activates and deactivates the Send All Calls feature for itself by using the send all calls feature access code.

The IP DECT system invokes or cancels Send All Calls for a remote station by dialing the Remote Send All Calls Activation or Deactivation feature access codes. To do this, you must have console permissions assigned to your Class of Service (COS) for the station.

Shuffling (IP direct connections)

The IP DECT configuration supports shuffling whenever the **Direct IP to IP Audio Connections** field is administered to y on the H.323 Signaling Group screen for X-mobility type of DECT.

SIP - Session Initiation Protocol

The IP DECT system is configured using H.323 IP trunks, not SIP trunks.

Station Firmware Download

The Station Firmware Download feature access code is not applicable, but you can download the firmware to the DECT stations in a different way. The 3720 and 3725 DECT handsets support automatic software download over the air (OTA) in combination with the Avaya In-Building Wireless Server (AIWS).

Station Lock

The IP DECT system locks or unlocks the stations by dialing the Station Lock Activation or Deactivation feature access codes.

Station Security Code Change

The IP DECT system changes their station security code by dialing the Station Security Code Change feature access code.

Team Button

The IP DECT can be a monitored station for the Team Button functionality.

Tenant Partition

An IP DECT station can be restricted to a specific Tenant Partition (TN).

Terminating Extension Group

An IP DECT station can be a member of a terminating extension group (as a primary, not a bridge).

Transfer

When the IP DECT station indicates a flash during a call, it must be treated as initiating a transfer operation. The operation can be a blind or supervised transfer, and includes display updates.

The IP DECT station can be used as the transferor or the transferee for the Transfer Recall feature.

The IP DECT station transfers a call directly to voice mail by dialing the Transfer to Voice Mail feature access code.

Trunks

The IP DECT system initiates a trunk call by dialing a Trunk Access Code (TAC).

The IP DECT station answers a call alerting on night bells by dialing the Trunk Answer Any Station feature access code.

Uniform Dialing Plan

The IP DECT system supports a Uniform Dialing Plan.

User Control Restriction

The IP DECT system changes the restriction levels for a specific user by dialing the User Control Restrict Activation or Deactivation feature access codes. To do this, you must have console permissions assigned to your Class of Service (COS) for the station.

Whisper Page

The IP DECT station sends a whisper page to another user by dialing the Whisper Page Activation feature access code. The IP DECT station can be the recipient of a Whisper Page call, but cannot control the Whisper Page feature through the Whisper Page Off or Answerback feature buttons, as the IP DECT stations cannot support administered feature buttons.

Chapter 109: ISDN Service

Use the Integrated Services Digital Network (ISDN) Service feature to provide a message-oriented signaling method by which information can be sent along with a call. The ISDN Service feature also gives you access to a variety of public and private network services and facilities.

The ISDN standard consists of Layers 1, 2, and 3 of the Open System Interconnect (OSI) model. Communication Manager can be connected to an ISDN by way of the standard frame formats: Basic Rate Interface (BRI) and the Primary Rate Interface (PRI).

Detailed description of ISDN Service

The ISDN Service feature provides end-to-end digital connections and uses a high-speed interface that provides service-independent access to switched services. Through internationally accepted standard interfaces, an ISDN provides circuit or packet-switched connections within a network, and can link to other ISDN-supported interfaces to provide national and international digital connections.

Note:

This feature description does not contain procedures for working with ISDN trunk groups. Due to the complexity of ISDN technology and the potential consequences of errors, ask your Avaya representative to help you in planning, installing, and administering ISDN trunks.

ISDN supports the following features:

- Call-by-Call Service Selection (CBC)
- Distributed Communications System (DCS). (Only ISDN-PRI supports DCS+ and DCS with Rerouting)
- Electronic Tandem Networks (ETN)
- Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS), but only with ISDN-PRI.
- Generalized Route Selection (GRS)
- Call Identification Display - Calling Party Number (CPN) and Billing Number (BN)
- Administered Connections and Access Endpoints
- Interworking, or the mixture of ISDN and non-ISDN trunks and stations

- Wideband Switching (H0, H11, H12, and NxDS0, but only with ISDN-PRI.
- QSIG Multivendor Connectivity
- Lookahead Interflow
- Lookahead Routing
- Usage Allocation

ISDN transmission rate and protocols

In ISDN-PRI, the transmission standard for Layer 1 (the physical layer) is either DS1 T1 or E1. The DS1 T1 (used in North America and Japan) is a digital-transmission standard that carries traffic at the rate of 1.544 Mbps, and the E1 (used in Europe) carries traffic at a rate of 2.048 Mbps. The D (data) channel multiplexes signaling messages for the B (bearer) channels carrying voice or data. In a T1, when a D-channel is present, it occupies Channel 24. In an E1, when a D-channel is present, it occupies channel 16.

Communication Manager offers several administrable protocols, each of which provides a different set of ISDN services. The following combination of services, including but not limited to Basic Call, Basic Supplementary Services, Supplementary Services with Rerouting, Display, and QSIG Networking are supported on the ISDN-PRI interface. Available services outside the United States vary from country to country.

With ISDN, Communication Manager interfaces with a wide range of other products including servers, network switches, and host computers. These products include earlier releases of servers running Communication Manager, public network switches (for example, AT&T 4ESS, Lucent 5ESS, and Northern Telecom DMS250), and other products adhering to the ISDN signaling protocol.

The figure on page 891 shows an example of how ISDN is used in private and public network configurations. For example, ISDN can be used to connect a switch to a public-switched network, to other switches, and to computers.

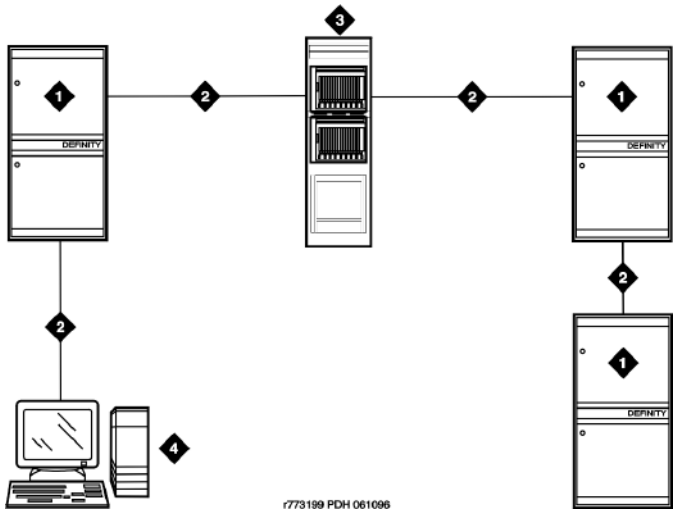


Figure 17: ISDN network configuration

Table 80: Figure notes:

1. Avaya Server
2. ISDN trunk
1. Public switched network
2. Host computer

AT&T Switched Network protocol

Communication Manager supports the AT&T Switched Network Protocol described in the TR41449 (for 4ESS to common carrier) and TR41459 (for 5ESS to CO) ISDN protocol standards as defined by AT&T. This protocol is used when the DS1 media module is administered for Country Code 1, Protocol Version a. The AT&T Switched Network provides you with the following services.

Access to AT&T Switched Network Services with ISDN

ISDN provides access to AT&T Switched Network Services. The definition of the **Service Type** field on the ISDN Trunk Group screen includes a table that outlines these switched-network services. An ISDN trunk group may be dedicated to a particular feature. Alternately, an ISDN call-by-call trunk group may provide access to several features.

ISDN Call Identification Display

ISDN Call Identification Display provides a transparent name and number display for all display-equipped telephones within an ISDN network. The feature is transparent in that the same information can be provided at all ISDN facilities. Telephones using this feature should be digital telephones with a 40-character alphanumeric display. The Merlin hybrid sets with 32-character displays (7315H and 7317H) also support this feature.

ISDN Call Identification Display is provided in addition to the normal Telephone Display and Attendant Display features when the network supports end-to-end ISDN connectivity. When both ISDN and DCS display information are received, either the DCS or ISDN call identification information can be displayed. If only ISDN display information is received, information displays in ISDN format.

The display fields that may be used for ISDN are **Name**, **Number**, **Miscellaneous Call Identification**, and **Reason for Call Redirection**. The display information varies, depending on the type of call, how the call is handled (for example, whether it is redirected or not), and the information is available on the call.

ISDN CPN/BN to Host Call Identification

The CPN/BN to Host Call Identification enables CPN and BN information to be passed from Communication Manager to the ISDN Gateway, so that the ISDN Gateway can forward the information to a host for data-screen delivery to agents in an ACD split.

By delivering call-identification information such as CPN/BN and additional Communication Manager information such as the answering-agent’s extension to an adjunct network (ISDN Gateway), the adjunct automatically delivers data screens to agents for new calls and call transfers.

The figure on page 893 shows a simplified diagram of a CPN- and BN-to-host arrangement. The ISDN Gateway is a UNIX or MS-DOS computer connected to Communication Manager on one side and to a host computer on the other side. The media server connection is over a synchronous interface with BX.25 protocol.

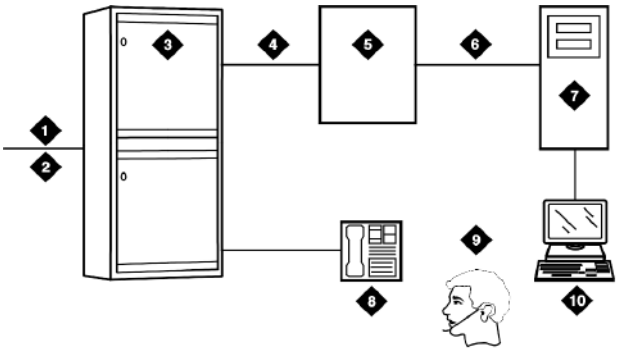


Figure 18: CPN- and BN-to-host configuration

Table 81: Figure notes:

1. ISDN trunk	1. Existing interface
2. SID/ANI	2. Host computer
3. Avaya Server	3. Telephone
4. BX.25	4. ACD agent position
5. ISDN Gateway	5. Data terminal

ISDN private network services

In addition to providing access to switched-public networks, ISDN provides private-network services by connecting Communication Manager in an ETN, DCS, or QSIG Network. This gives you more efficient private networks that support new integrated voice and data services. ETN, DCS, and QSIG networking services are provided as follows.

ETN services with ISDN

Avaya S8XXX Servers that function as tandem nodes in an ETN can be interconnected using DS1 trunking facilities with ISDN. All signaling between the tandem switches is done with ISDN D-channel and normal ISDN protocol. The ISDN can also be used to connect ETN tandem and main servers or switches. In this case, the main server or switch collects all of the address digits from local users as well as users at other satellite and tributary switches, and originates a call over ISDN to the tandem server or switch.

Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) are used with ISDN and DS1 trunking facilities to access ETN facilities. AAR and ARS are used to collect the dialing information for the call that is originated from the main server or switch.

DCS services with ISDN

ISDN-PRI facilities can be used in a DCS arrangement whenever tie trunks are used to connect the DCS nodes. Most DCS features are not affected by ISDN-PRI. However, there is a minor impact on a few of the DCS features, as far as the functions that the local and remote media servers or switches perform.

QSIG services with ISDN

QSIG networking provides compliance to the International Organization for Standardization (ISO) ISDN private-networking specifications. The QSIG Networking platform is supported over the ISDN Basic Call setup protocol. Communication Manager supports QSIG Supplementary Services.

Wideband Switching (ISDN-PRI only) with ISDN

Wideband Switching provides support for services that require large bandwidth, such as high-speed video conferencing. Wideband also supports multiple channel calls end-to-end. These services have traditionally been handled by dedicated facilities. With Wideband Switching, dedicated facilities are no longer a requirement for these large bandwidth services.

Call-by-Call Service Selection with ISDN

The same ISDN trunk group uses Call-by-Call Service Selection to carry calls to a variety of services or facilities. Embodied in this feature is the ability to allocate usage. It provides significant flexibility for creating user-defined incoming and outgoing services and is used on any ISDN trunk group.

Access to Software Defined Data Network

With ISDN, the SDDN service may be accessed. SDDN provides virtual private-line connectivity by way of the switched public network. The services provided by SDDN include voice, data, and video applications. SDDN services complement the ISDN voice services.

Access to Switched Digital International

Switched Digital International (SDI) provides 64 kbps of unrestricted connectivity to international locations by way of the AT&T Switched Network. It is also the backbone for the AT&T International ISDN network. SDI complements the ACCUNET digital service already available to United States locations. This service can be accessed using Call-by-Call Service Selection. SDI provides economical high-speed data transfer to international locations.

National ISDN-2 services

Communication Manager supports National ISDN-2 (NI-2), which offers many of the same services as the AT&T Switched Network protocol. The NI-2 protocol is used when the DS1 media module is administered for Country Code 1, Protocol Version b.

NI-2 provides users with the following services:

- Calling Line Identification

- Non-Facility Associated Signaling (ISDN-PRI only)
- D-Channel Backup, but with ISDN-PRI only
- Wideband Switching, but with ISDN-PRI only
- Call-by-Call Service Selection

ISDN-2 Calling Line Identification

Calling Line Identification for NI-2 is essentially CPN identification, as previously described.

ISDN-2 Non-Facility Associated Signaling (ISDN-PRI only)

An ISDN-PRI T1 or E1 Interface uses Non-Facility Associated Signaling (NFAS) D-channel (signaling channel) to convey signaling information for B-channels (voice and data) on ISDN-PRI T1 or E1 facilities other than the facility that contains the D-channel.

ISDN-2 D-Channel Backup (ISDN-PRI only)

D-Channel Backup is provided to improve reliability in the event of a signaling-link failure.

ISDN-2 Wideband Switching (ISDN-PRI only)

Wideband Switching for NI-2 is essentially the same as that of the AT&T Switched Network ISDN-PRI protocol.

ISDN-2 Call-by-Call Service Selection

Call-by-Call Service Selection for NI-2 is essentially the same as that for the AT&T Switched Network ISDN-PRI protocol.

ISDN interworking

Using ISDN interworking, you can have a combination of both ISDN and non-ISDN trunking and station facilities. A non-ISDN trunking facility is any trunk facility supported by the system that does not use the ITU-T recommended Q.931 message set for signaling. Non-ISDN trunking facilities include facilities such as analog trunks, AVD DS1 trunks, and DS1 trunks with bit-oriented signaling (robbed-bit or common channel).

Communication Manager supports the conversion of ISDN signaling to non-ISDN in-band signaling and the conversion of non-ISDN in-band signaling to ISDN signaling for interworking purposes.

A mixture of ISDN and non-ISDN signaling is required to provide end-to-end signaling when using different types of trunk or station facilities on a call. The figure on page 896 shows an example of interworking.

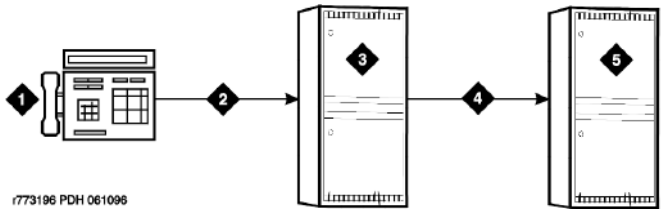


Figure 19: ISDN and non-ISDN interworking

Table 82: Figure notes:

1. Call from network to system B
2. ISDN trunk
3. System A
1. Non-ISDN trunk
2. System B

In this example, a call for someone at Switch B comes into Switch A. Using Interworking, the ISDN signaling of the call can be converted at Switch A to non-ISDN in-band signaling before the call forwards to Switch B. Even though the call comes into Switch A on an ISDN trunk, Switch A can send the call to Switch B over a non-ISDN trunk by converting the signaling information.

The system provides accurate CDR billing information on calls that are not interworked. Accuracy of CDR billing information on interworked calls is equivalent to the accuracy provided by the public network.

Communication Manager supports sending a non-ISDN trunk name as the connected name. Therefore, a non-ISDN trunk name can be sent as the connected name even when a call starts out as an ISDN call but is interworked over non-ISDN trunks.

ISDN Call Identification Display overview

Two types of identification numbers are provided with ISDN and may be used in the various types of displays used with ISDN. The two types of identification numbers are as follows:

- Calling Party Number (CPN): A 0-15 digit DDD number associated with a specific station. When a system user makes a call that uses ISDN, that user's CPN is provided by the system for ISDN. ISDN public-unknown numbering or ISDN private numbering screens are administered to create a 0-15 digit CPN from a local station number.
- Billing Number (BN): The calling party's billing number, which is provided to an inter-exchange network by way of Equal Access or CAMA. This number is stored at either a local or network switch. If a customer is connected directly to the AT&T Switched Network, the BN is the customer's billing number stored in that network. If the CPN is not provided on an incoming ISDN call, the network uses the BN for the station identification number.

The following types of display information are provided with ISDN:

- Calling party's number

  The called party's screen displays the calling party's number. This number is provided only if the outgoing ISDN trunk group is administered to send the CPN, and if ISDN public-unknown numbering or ISDN private numbering screens are administered to create a CPN. On calls incoming to a system, the network may provide either the CPN or BN as the calling party's

number. Extensions and 12-digit international numbers display without dashes. Dashes are only used for 7-digit and 10-digit numbers when North American Area Code is enabled on the Dial Plan screen.

- Calling party’s name

  The called party's screen displays the calling party’s name. On calls generated from a DEFINITY server, the caller’s name is provided if the ISDN trunk group is administered to send the name to the network. On calls incoming to a DEFINITY server, the (public or private) network may provide the caller’s name. If the caller’s name is unavailable, the called party’s display shows “CALL FROM” instead, followed by the calling party’s number (if available).

- Connected party’s number

  The caller's screen displays the connected party’s number. On calls generated from a DEFINITY server, callers’ displays may show the digits dialed as the call is made. If the (public or private) ISDN network provides the connected party’s number, the calling party’s display is updated to show the connected party’s number. The format of the connected party’s number is the same as that of the calling party’s number described previously on calls incoming to a DEFINITY server. The 0-15 digit number of the party who answers the call is provided to the ISDN network only if the incoming ISDN trunk group is administered to send connected number to the network and ISDN public-unknown numbering or ISDN private numbering screens are administered to create a CPN.

  Note:

  The connected party may be the party actually called, in the event the call is transferred before the connected party answers the call.

- Connected party’s name

  The caller's screen displays the connected party’s name. On calls generated from a DEFINITY server, the (public or private) ISDN network may provide the connected party’s name to the Communication Manager, when the call is answered. If the connected party’s name is unavailable, the calling party’s display shows ANSWERED BY, followed by the connected party’s number (if available).

  On calls incoming to a DEFINITY server, the connected party’s name is provided if the incoming ISDN trunk group is administered to send the name to the network.

Depending on how the media servers or switches that are involved in a call are configured, parties may see none, some, or all the information described above.

ISDN displays for redirected calls

Features such as Call Coverage, Call Forwarding All Calls, Bridged Call Appearance, or Call Pickup redirect calls from the called party’s extension to some other destination. Once the redirected call has been connected at its new destination, the displays for the calling, called, and connected parties are as follows:

Calling party display

a= CONNECTED NAME CONNECTED NUM MISCID

Called party display

This is the display of the party the caller originally dialed. If this party bridges onto the redirected call after it has been answered, they see:

a= CONFERENCE 2

In this situation, the connected party's display (see below) shows the same information. The calling party's display is also updated if the calling and called parties are on the same server running Communication Manager.

Connected party display

The connected party is the party who answers the redirected call.

a= CALLING ID to CALLED ID R

The R indicates the reason for redirection. The CALLING ID and the CALLED ID may be the name or the number, depending on the information received from the far end.

ISDN displays for conference calls

Both terminal and attendant conference calls are identified as calls with "n" number of conferees. This display information generates locally and does not change the display shown by another server. If the conference call eventually drops back to a two-party call, the original display information is restored. However, when two DCS and/or ISDN calls (or any possible combination of each) are conferenced and revert to a two-party call, the trunk group of the remaining call displays.

ISDN displays for calls to hunt groups

On ISDN calls to a hunt group extension, the caller's display identifies either the name of the hunt group or the name of the group member who answers the call, depending on hunt group administration.

ISDN displays for calls to Terminating Extension Groups

On ISDN calls to a Terminating Extension Group (TEG), the caller's display identifies either the group or the group member who answers the call, depending on administration.

ISDN Caller Information Forwarding

With CINFO you can use a vector collect digits step to retrieve caller entered digits (ced) and customer database-provided digits (cdpd) supplied by the network in an incoming call's ISDN SET UP message. ISDN is required if the CINFO comes from the network.

ISDN Facilities Restriction Level and traveling class mark

The traveling class mark (TCM) used to pass on the originating facilities's restriction level (FRL) is sent by ISDN facilities in the SETUP message only if the trunk services type is tandem.

ISDN Information Indicator Digits (II-digits)

With II-digits you can make vector-routing decisions based on the type of the originating line. II-digits are provided for an incoming call by ISDN-PRI. It is a generally available ISDN AT&T Network service.

Malicious Call Trace with ISDN

ISDN calling number identification is sent when Malicious Call Trace (MCT) notification is activated on an ISDN trunk.

ISDN Multiple Subscriber Number - Limited

The ISDN standard Multiple Subscriber Number (MSN) feature lets you assign multiple extensions to a single BRI endpoint. A side effect of supporting the NT interface is the MSN feature works with BRI endpoints allowing the Channel ID IE to be encoded as preferred. The endpoint must be administered as the far end of an NT-side ISDN-BRI trunk group. Also, you must use the Uniform Dial Plan (UDP) feature to assign the desired extensions to the node at the far end of the trunk group.

Overlap Sending with ISDN

You can administer overlap sending on AAR and ARS calls routed over ISDN trunk groups. You can send and receive one digit at a time instead of enbloc. (With enbloc, digits are not sent until the entire group of digits is received).

TGU/TGE trunks and ISDN (Italy) Interworking

This modifies ISDN messaging operations in systems that use TGE/TGU trunks to network satellite servers or switches. Messaging from Communication Manager provides appropriate ringback or busy tone to the calling party.

ISDN Service administration

This section describes the screens that you use to administer the ISDN Service feature.

Screens for administering ISDN Service

Screen name	Purpose	Fields
Access Endpoint	Administer ISDN Service.	• Access Endpoints • Wideband Access Endpoint
Trunk Groups	Administer incoming calls and trunk groups usage and allocation.	All
ISDN Numbering - Private	Administer private numbering plans.	All

Table continues…

Screen name	Purpose	Fields
ISDN Numbering - Public/ Unknown	Administer ISDN call identification displays.	All

Interactions for ISDN Service

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

Australia Malicious Call Trace (MCT)

Communication Manager with a BRI connection to the Australian public network can notify the network if a user in a private network invokes the MCT feature. This service works on Australian national connections.

Direct Inward Dialing (DID)

Some public network operators may not offer full DID service on BRI trunks, but instead may offer the BRI equivalent, which typically is called MSN. This is the case if the public network treats the BRI as an endpoint interface rather than a trunk group interface. In such a case, the network only routes up to 10 public numbers to a particular pair of BRI trunks. The network may not let calls overflow from one BRI trunk to another.

D-Channel Backup

D-Channel Backup is not supported on BRI connections.

Distributed Communications System

If both DCS and ISDN features are provided over the same facility with a DEFINITY server, DCS displays generally override ISDN displays. However, with Communication Manager, the ISDN connected name and number can override the DCS called name and number if the **Display Connected Name/Number for ISDN DCS Calls** field is y on the Feature-Related System Parameters screen.

BRI trunks support DCS if using a BX.25 link to transport the DCS messages. DCS+, also known as DCS Over ISDN D-Channel, according to the AT&T protocol, is not supported on BRI trunks.

Facility Test Calls

Neither BRI or PRI trunks support Facility Test Calls.

France VN4 Protocol

The France national VN4 protocol is supported on BRI trunks as ETSI.

Generalized Route Selection

BRI trunks are capable of carrying 56Kbps or 64Kbps data calls. The link coding that restricts certain PRI trunks to 56Kbps only does not apply to BRI trunks.

German 1TR6 Protocol

The German national 1TR6 protocol is not supported over BRI trunks.

Message Sequence Tracer

ISDN-BRI trunks support Message Sequence Tracer. However, certain filtering capabilities available for PRI trunks are not available. You cannot filter BRI trunk messages based on incoming/outgoing calling/called number.

Network Access - Public (LEC/AT&T/Other Carriers)

Public network access using BRI trunks is available but only in those countries that support point-to-point BRI connections. In the U.S., BRI access is offered only by the Local Exchange Carriers and not by Interexchange Carriers.

Network Access - Private Premises Based

Full support for private-network connections using BRI trunks is available.

Non-Facility Associated Signaling

Non-Facility Associated Signaling is not supported on BRI connections.

Temporary Signaling Connections

Communication Manager does not support Temporary Signaling Connections according to the AT&T protocol on BRI trunk interfaces. Only the QSIG NCA TSC protocol is supported on these interfaces

Wideband Switching (NxDS0)

Communication Manager does not support wideband switching on BRI connections.

Chapter 110: Last Number Dialed

Use the Last Number Dialed feature to automatically redial the last telephone number that was dialed from the telephone, or from a bridged appearance of the telephone.

Detailed description of Last Number Dialed

With the Last Number Dialed feature, users can to automatically redial the last telephone number that was dialed from the telephone, or from a bridged appearance of the telephone.

The system saves the first 24 digits of the last telephone number that was dialed. The system saves the digits for calls that the user places with either manual dialing or Abbreviated Dialing. When a user presses the **Last Number Dialed** button, or dials the Feature Access Code (FAC) for Last Number Dialed, the system places the call again.

Last Number Dialed administration

This section provides the screens that you need to administer the Last Number Dialed feature:

Screens for administering Last Number Dialed

Screen name	Purpose	Fields
Attendant Console	Assign the last-numb feature button to an attendant console.	Any available button field in the **Feature Button Assignments** area
Feature Access Code (FAC)	Assign a FAC for Last Number Dialed.	Last Number Dialed Access Code
Station - multiappearance	Assign the last-numb feature button for a user.	Any available button field in the **Button Assignments** area

Considerations for Last Number Dialed

This section provides information about how the Last Number Dialed feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Last Number Dialed under all conditions. The following considerations apply to Last Number Dialed:

- When the user presses the last number dialed button, the system outpulses any special characters that are stored in the **Abbreviated Dialing** button that was used to place the previous call. Such characters include Pause, Wait, Mark, and Suppress.
- Any delays that a user might encounter when the user dials the call manually, are not repeated when the user uses the Last Number Dialed feature.
- The system does not save Last Number Dialed information to disk, tape, or flash card. The system never saves manually dialed end-to-end, signaling digits.
- A user can enter a partial number, disconnect the call, and use Last Number Dialed, and then manually enter the remaining digits. If the user calls from a display telephone, the system does not display the digits that the user enters manually. However, the system completes the call.

Interactions for Last Number Dialed

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

Abbreviated Dialing

If the previously called number is in an Abbreviated Dialing privileged list, and the Class of Restriction (COR) of the user prevents the user from dialing the number, the system uses Intercept Treatment when the user presses Last Number Dialed. To redial the number, the user must again use the Abbreviated Dialing privileged list.

Automatic Callback

Users can use Automatic Callback after the users use Last Number Dialed on a call to an internal telephone.

Bridged Call Appearance

Last Number Dialed causes the last number that was dialed from a telephone, or a bridged appearance of the telephone, to be redialed.

Centralized Attendant Service (CAS)

If a CAS attendant attempts to extend a call with Last Number Dialed, the system does not complete the call.

Chapter 111: Leave Word Calling

Using the Leave Word Calling (LWC) feature, internal system users can leave a short pre-programmed message for other internal users. When the message is stored, the Automatic Message Waiting lamp lights on the called telephone. Users can retrieve LWC messages on a telephone display, Voice Messaging Retrieval, or the AUDIX system. Messages can be retrieved in English, French, Italian, Spanish, or a user-defined language.

Detailed description of Leave Word Calling

LWC electronically stores a standard message. For example:

CARTER, ANN 2/7 10:45a 2 CALL 3124

This message means that Ann Carter called two times, the last time on the morning of February 7 at 10:45 a.m. She wants a return call to extension 3124.

When the system receives identical messages, the system updates only the date and the time, and number of messages. If nine or more identical messages accumulate, the count remains at nine, and the system updates only the date and time.

Messages can be stored by calling users, called users, and covering users as follows:

A caller who leaves a LWC message can cancel that message, if the message was not already retrieved. To cancel the message, the calling user lifts the handset, presses LWC Cancel or dials the access code, and then dials the extension of the called party.

The system can indicate that one telephone received a LWC message on a second telephone. The system lights a remote Automatic Message Waiting lamp at the remote telephone and the Automatic Message Waiting lamp lights at the called voice terminal. The Remote Automatic Message Waiting lamp is a status lamp associated with a button assigned for this purpose. Thus, the lamp on an assistant's telephone can light when an executive receives a LWC message. If the executive calls to retrieve messages, the assistant knows at a glance if any messages were left.

Users without Voice Terminal Display can have their messages retrieved by a system-wide message retriever or by covering users in their Call Coverage path. They can also use Voice Message Retrieval.

With the Leave Word Calling Log External Calls capability, the system can monitor unanswered calls. The server keeps a record of as many as 15 calls, provided that the caller identification is

available, and the message lamp on the telephone lights. The display on the telephone shows the names and numbers of unsuccessful callers.

The system restricts unauthorized users from displaying, canceling, or deleting messages. The Lock capability restricts a voice terminal and the Unlock function releases the restriction. To activate Lock, the users dial a system-wide access code. They cancel Lock by first dialing a system-wide access code and then an Unlock security code unique to the voice terminal. These functions apply only to the voice terminal where the function is active. You can assign a status lamp to show the lock status of the voice terminal.

End-user procedures for Leave Word Calling

Leaving an LWC message

Procedure

1. Press the **LWC** button or dial the LWC access code.
2. Dial the required number.
3. Before the call is answered, if you are a multiappearance voice-terminal user, press **LWC**.

   If you are a single-line voice-terminal user, press **Recall** and dial the access code.
4. After the call is answered, press **LWC** or **Recall** and dial the access code.

Responding to an LWC message

Procedure

1. The user answers the call.
2. The called user presses LWC to leave a message for the calling user to return the call.
3. A called user can store an LWC message by dialing the LWC access code only if the called user has an analog voice terminal.

Responding to an LWC message from coverage

Procedure

1. The covering user answers the call.
2. The covering user presses **Coverage Callback** to store a message for the called user that tells them to return a call the calling user.
3. After answering the call, the covering user presses **LWC** to leave a call-me message for the originally called user.

   In addition, a user that was placed on hold can activate LWC and leave a message for the holding user to place a return call.

Considerations for Leave Word Calling

This section provides information about how the Leave Word Calling (LWC) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Leave Word Calling feature under all conditions. The following considerations apply to the Leave Word Calling feature:

- You can administer up to 10 telephones, or nine telephones and the attendant console group as system-wide message retrievers.
- If the stored-message level reaches 95% of capacity, the status lamps that are associated with all Coverage Message Retrieval buttons in the system flash. These lamps continue to flash until the stored-message level falls below 85%. Authorized retrievers can selectively delete messages to gain storage space. The system does not automatically purge old messages.
- LWC messages cannot be stored, canceled, or retrieved for Vector Directory Number extensions.

Interactions for Leave Word Calling

This section provides information about how the Leave Word Calling (LWC) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Leave Word Calling in any feature configuration.

AUDIX Interface

LWC Cancel cannot be used to cancel an AUDIX message.

Bridged Call Appearance

A LWC message that is left by a user on a bridged call appearance leaves a message for the called party to call the primary extension for the bridged call appearance. When a user calls a primary extension and activates LWC, the message is left for the primary extension, even if the call was answered at a bridged call appearance.

Call Coverage

You can use LWC with or without Call Coverage. However, the two features complement each other. LWC provides the Coverage Callback option. Also, a caller can activate LWC for the called party even if the call was answered by a covering user.

Centralized Attendant Service (CAS)

LWC Message Retrieval does not work with CAS.

Conference

A member of a conference call cannot activate LWC because the user cannot be uniquely identified. After LWC is activated for a party on a conference or transfer, the origination of the conference or the transfer cannot press Conference/Transfer a second time to return to the

original call. The originator must select the call appearance button to return to the previously held call.

Distributed Communications System (DCS)

LWC works with DCS, but only for 4- digit and 5-digit extension dial plans. LWC works with QSIG for all dial plans of 3- through 7-digits.

Expert Agent Selection (EAS)

When an EAS agent is logged into a telephone, the agent can only retrieve LWC messages that are left for the login ID of the agent. To retrieve LWC messages that are left for that telephone, the agent must log out.

When an EAS agent is logged into a telephone, the Message lamp of the telephone defaults to tracking the status of LWC messages waiting for the telephone. However, you can assign the Message lamp to track the status of LWC messages waiting for the login ID of the agent.

Message Waiting Indicator (MWI)

As QSIG does not specify a standard way to light the MWI lamp upon receipt of an LWC message, systems running Communication Manager must work properly.

Vector Directory Number (VDN)

LWC messages cannot be stored, cancelled, or retrieved through VDN extensions.

Chapter 112: Line Lockout

Use the Line Lockout feature to remove a user with a single-line telephone from service when the user does not disconnect after the user receives dial tone or intercept tone.

Detailed description of Line Lockout

Lockout occurs when:

- A user does not disconnect after the other party on a call disconnects.
  - The user receives the dial tone for 10 seconds, and then receives the intercept tone for the interval that you administer.
  - You can administer the system to play a special howler tone before the system takes the telephone out of service.
  - If the handset remains off-hook, the system takes the telephone out of service.
- A user pauses for 10 seconds between digits when the user dials numbers.
  - The user receives intercept tone for 30 seconds.
  - If the handset remains off-hook, the system takes the telephone out of service.

The telephone remains out of service until the user disconnects.

Line Lockout administration

This section describes the screens that you use to administer Line Lockout.

Screens for administering Line Lockout

Screen name	Purpose	Fields
Feature-Related System Parameters	Specify the number of seconds that the system waits before the system removes the telephone of the user from service, after the system generates the warning tone.	Line Intercept Tone Timer
	Specify the tone that the system generates for the last user on a call, until the user disconnects or the system generates the tone for 45 seconds.	Station Tone Forward Disconnect
	Specify the number of seconds that the system supports for a telephone with an Off-Hook Class of Service (COS) to remain off-hook before the system sends an emergency call to the attendant.	Time Before Off-hook Alert
System Parameters Country-Options	Enable the system to disconnect calls that are unanswered	Disconnect on No Answer by Call Type
	Enable the system to generate howler tone for users, before the system removes the telephone of the user from service.	Howler Tone After Busy

Considerations for Line Lockout

This section provides information about how the Line Lockout feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Line Lockout under all conditions. The following considerations apply to Line Lockout:

- The out-of-service condition that Line Lockout provides does not tie up switching facilities.
- Line Lockout does not apply to multiappearance telephones.

Chapter 113: Listed Directory Number

Using the Listed Directory Numbers (LDN) feature, outside callers can access your attendant group.

Listed Directory Number supports the following capabilities:

- Attendant group access through incoming Direct Inward Dialing (DID) trunks
- Attendant group access through incoming central office (CO) and foreign exchange (FX) trunks

Detailed description of Listed Directory Number

The system routes both incoming Direct Inward Dialing (DID) calls and incoming foreign exchange (FX) and central office (CO) calls to an attendant group, based on how you administer the trunks.

LDN routing of incoming DID trunk calls

DID calls can only reach extensions. Using the LDN feature, you can assign one or more extensions to an attendant group. The system uses the LDN extension or extensions to route DID calls to an attendant group.

LDN routing of incoming FX and CO trunk calls

Incoming FX and CO trunks calls can terminate at an attendant group. You can also administer your system to terminate an incoming FX or CO trunk to an:

Attendant group

If you decide to terminate the call at an attendant group, the system processes the call as an LDN call.

Extension

The extension can be a vector directory number (VDN), an Automatic Call Distribution (ACD) split, a Direct Department Calling (DDC) group, a Uniform Call Distribution (UCD) group, a remote access extension, or any system extension.

Listed Directory Number administration

The following tasks are part of the administration process for the Listed Directory Number (LDN) feature:

- Assigning listed directory numbers
- Assigning an incoming destination to a trunk for LDN

Related links

Assigning listed directory numbers on page 911
Assigning an incoming destination to a trunk for LDN on page 912

Screens for administering Listed Directory Number

Screen name	Purpose	Fields
Listed Directory Numbers	Assign listed directory numbers and an optional, night-service destination.	All
Trunk Group	Assign an incoming destination to a trunk.	Incoming Destination

Assigning listed directory numbers

Procedure

1. Enter `change listed-directory-number`.
2. In the **Night Destination** field, type a night destination extension that consists of 1 to 8 digits.

   The extension must be comprised of the numbers 0 through 9. The night destination extension receives the calls to the extensions that you type in the **Ext** field, when the Night Service feature is active.
3. In the **Ext** field, type the number of the extension that you want to use for the LDN feature.

   The extension number can consist of 1 to 16 digits.
4. In the **Name** field, type the name that you use to identify the listed directory number.

   The name can consist of 1 to 27 alphanumeric characters.
5. In the **TN** field, type the Tenant Partition number.
6. Repeat Steps 3 through 5 for each extension to which you want to assign a listed directory number.
7. Press `Enter` to save your changes.

Assigning an incoming destination to a trunk for LDN

Procedure

1. Enter `change trunk-group n`, where *n* is the number of the trunk group to which you want to assign an incoming destination.
2. In the **Incoming Destination** field, perform one of the following actions:
   - If the **Trunk Type** field on the Trunk Group screen is not set to auto, leave the field blank.
   - Type the extension for the incoming calls.

     You can type any extension. However, the extension is usually for a VDN, a voice response unit, or a voice messaging system. The Night Service feature overrides the extension that you type in the **Incoming Destination** field.

     Caution:

     When you assign a Multi-Location Dial Plan shortened extension in a field that is designed for announcement extensions, certain administration end validations that are usually performed on announcement extensions are not performed, and resultant warnings or submittal denials do not occur. The system does not display shortened extensions in any display or a list that shows announcement extensions. Ensure that you administer the correct type of announcement for the application when you assign shortened extensions.
   - If you want the system to route the calls to the attendant, type `attd`.

     The system records the calls as LDN calls on the call detail recording records.

     The system displays the **Incoming Destination** field on the CO Trunk screen, when the **Direction** field on the Trunk Group screen is set to incoming or two-way.

     Use the **Incoming Destination** field to set the destination for all incoming calls on trunk groups such as central office (CO), foreign exchange (FX), and Wide Area Telecommunications Service (WATS), that must terminate at a single destination. This field can be set to a station so all incoming calls will ring at this station. If this destination station is busy, the caller will hear a ringback tone instead of a busy tone. The destination that you type in the **Incoming Destination** field is also the default night service destination, unless you enter a different destination in the **Night Service** field.
3. Press `Enter` to save your changes.

Considerations for Listed Directory Number

This section provides information about how the Listed Directory Number (LDN) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits

of Listed Directory Number under all conditions. The following considerations apply to Listed Directory Number:

- The number of listed directory numbers that you can assign depends on the configuration of your system.

Interactions for Listed Directory Number

This section provides information about how the Listed Directory Number (LDN) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Listed Directory Number in any feature configuration.

Night Service

If you activate the Night Service capability, and a night console is not assigned or is not operational, the system routes:

- Incoming Direct Inward Dialing (DID) LDN calls route to a designated DID LDN night extension. If no DID LDN night extension is designated, the system routes DID LDN calls to the attendant
- Incoming central office (CO) or foreign exchange (FX) trunk calls to the night destination that is specified for the trunk group. If no night destination is specified for the trunk group, the system routes the calls to the normal incoming destination for that trunk group.
- Internal calls and coverage calls to the attendant to the DID LDN night extension during night service.

Call Coverage and Tenant Partitioning

If a covered call does not route to an attendant in the first tenant group, you can route it to an attendant group of a different tenant partition. For example, you can reroute a call to Tenant Group B if the call is to cover to an attendant for Tenant Partition A but does not route to the attendant or is received out of hours when Attendant Group A is unstaffed.

To reroute the covered calls to another tenant attendant group, Tenant Attendant group B in this example,

1. In the vector for the tenant A attendant vectoring VDN, add a failure branch to a **route-to ldn_number with cov y if unconditionally** step for the LDN extension for the tenant group B TN number.
2. Set the **with coverage** parameter of the route-to step must be set to **cov y** because the calls are covered. Else, the calls don’t route to the VDN. Also, set the **Cvg Enabled for VDN Route-to party?** field of original coverage path, which covers to Tenant A Attendant vectoring VDN, to **y**.

Chapter 114: Limit Number of Concurrent Calls

You can use the Limit Number of Concurrent Calls (LNCC) feature on a multiappearance station to restrict the number of incoming calls to one call at a time. If you enable the LNCC feature and the station user is busy, the subsequent incoming calls receive a busy tone.

With Communication Manager Release 6.3 or later, you can enable LNCC on 96x1 SIP stations.

A typical Communication Manager station has three call appearances. The first two call appearances are used for receiving calls, and the last call appearance is reserved for making calls or receiving priority calls, provided the **Restrict Last Appearance** is set to `y`.

However, LNCC allows:

- Outgoing calls, incoming priority calls, and emergency callback for SIP stations.
- Outgoing calls, incoming priority calls, emergency callback, and crisis alert for H.323 and DCP stations.

Related links

Enhancements to LNCC on page 915
Assigning the LimitInCalls button to H.323 and DCP telephones on page 915
Assigning the LimitInCalls button to SIP telephones on page 915
Assigning FAC for LNCC on page 916
Activating the LNCC feature on page 916
Deactivating the LNCC feature on page 917
Configuring the coverage path for LNCC on page 917
Viewing the status of the LNCC feature on page 917
Interactions for Limit Number of Concurrent Calls on page 918

Enhancements to LNCC

In Communication Manager Release 5.2 or later, a call to a station that is LNCC-busy is treated like a normal busy station. The call follows the call coverage path for the busy status in the following conditions:

- A station that has LNCC activated will follow a coverage path. The user does not hear a busy tone. The coverage path can be administered.
- The call hunts for a station per the administered coverage path if LNCC is activated in Hunt to Station mode.

To administer or view the coverage path for LNCC-busy, use the **change coverage path** *n* command or the **display coverage path** *n* command, where *n* indicates the number of the coverage path assigned to the station. For more information, see Creating a coverage path.

To administer or display the hunt-to station, use the **change station** or **display station** command.

Related links

Limit Number of Concurrent Calls on page 914
Creating a coverage path on page 368

Assigning the LimitInCalls button to H.323 and DCP telephones

Procedure

1. Type `change station n`, where *n* is the extension of the telephone on which you want to add the button, and press `Enter`.
2. On the Button Assignments page, type `limit-call` in a blank field, and press `Enter`.
3. Save the changes.

   The **LimitInCalls** button is displayed on the telephone.

Related links

Limit Number of Concurrent Calls on page 914

Assigning the LimitInCalls button to SIP telephones

Procedure

1. Log on to the System Manager web console.
2. Click **Elements** > **Communication Manager**.

3. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
4. Select the Communication Manager instance.
5. Click **Show List**.
6. Select the endpoint that you want to edit from the **Endpoint List** section.
7. Click **Edit**.
8. Click the **Button Assignments** tab.
9. Assign the **limit-call** button to the station.
10. Click **Commit** to save the changes.

    The **LimitInCalls** button is displayed on the telephone.

Related links

Limit Number of Concurrent Calls on page 914

Assigning FAC for LNCC

Procedure

1. Type `change feature-access-codes`, and press `Enter`.

   The system displays the Feature Access Codes screen.
2. In the **Limit Number of Concurrent Calls Activation** field, type the access code that you want to use to activate the LNCC feature.
3. In the **Deactivation** field, type the access code that you want to use to deactivate the LNCC feature.
4. Save the changes.

Related links

Limit Number of Concurrent Calls on page 914

Activating the LNCC feature

Procedure

On the telephone, perform one of the following:

- Dial the Limit Number of Concurrent Calls Activation FAC.
- Press the **LimitInCalls** button.

On activation, the system displays the **Limit Concurrent Incoming Calls** message on the DCP and H.323 stations while the station is idle.

Related links

Limit Number of Concurrent Calls on page 914

Deactivating the LNCC feature

Procedure

On the telephone, perform one of the following:

- Dial the Limit Number of Concurrent Calls Deactivation FAC.
- Press the **LimitInCalls** button.

The LNCC feature is deactivated on the telephone.

Related links

Limit Number of Concurrent Calls on page 914

Configuring the coverage path for LNCC

Procedure

1. Type `change coverage path n`, where *n* is the coverage path number of the station, and press `Enter`.

   The system displays the Coverage Path screen.
2. In the **Coverage Criteria** section, in the **Busy** field, type `y`.
3. In the **Coverage Points** section, in the **Point** fields, type the extensions, the hunt group number, or the coverage answer group numbers that you want as coverage points.
4. Save the changes.

Related links

Limit Number of Concurrent Calls on page 914

Viewing the status of the LNCC feature

Procedure

Type `status station n`, where *n* is the extension, and press `Enter`.

The system displays the General Status screen.

The value in the **Limit Incoming Calls** field displays the status of the LNCC feature:

- **no** indicates that the feature is deactivated.
- **yes** indicates that the feature is activated.

Related links

Limit Number of Concurrent Calls on page 914

Interactions for Limit Number of Concurrent Calls

Logged in agent call with LNCC active

A logged-in agent can activate or deactivate the LNCC feature for the enterprise user associated with the appliance. If an agent logs in to an LNCC-active appliance, or the logged-in agent activates LNCC, LNCC applies to the calls directed to the agent.

Auto Callback

When a call is made to a user who has LNCC activated, and the caller activates the Automatic Callback (ACB) feature, the caller receives an Automatic Callback call when the user becomes available.

The system treats the Automatic Callback call as a priority call. Therefore, an LNCC-active station that is busy receives the Automatic Callback call.

Bridged Call Appearance

If the LNCC-active primary station is busy, the Bridged Call Appearance features do not receive further calls to the primary station.

If an LNCC-active station is busy on a bridged call appearance, the subsequent calls to the primary call appearance of the station receive a busy tone. However, if the LNCC-active station is busy on a primary call appearance, the station receives the bridged calls.

Call Coverage

If an LNCC-active station is busy and does not have call coverage configured, the subsequent calls to the station receive a busy tone. However, if you configure the call coverage for the LNCC-active station, the subsequent calls to the station follow the coverage path. You can configure an LNCC-active station as a coverage point. However, if the station is busy, the system treats the station as an unavailable coverage point.

Group Termination

If an LNCC-active station is a member of a group, LNCC applies to group calls also. Therefore, if the LNCC-active member is busy, the station does not receive the group calls. If an LNCC-active station is busy on a group call, a station making a call to the LNCC-active station receives a busy tone.

Hold

The user of an LNCC-active station can put a call on hold. LNCC-active station places a call on hold, the station that has the call on hold receives a busy tone.

Crisis Alert

The system alerts an LNCC-active station with the crss-alert button assigned when an emergency call is initiated, even if the station is busy. From Communication Manager Release 8.1, SIP stations support Crisis Alert feature for J100 series phones.

E911 Callback

The user of an LNCC-active station can receive Emergency Callback even if the station has one or more appearances busy. However, the station must have an idle appearance to terminate the call.

Multiple Level Precedence Preemption

When an LNCC-active station is busy on a call, the system performs one of the following actions on an incoming MLPP call:

- If the precedence level of the MLPP call is higher than the active call, the system preempts the active call and the station receives the MLPP call.
- If the precedence level of the MLPP call is equal to or lower than the active call, the system activates call waiting on the active call, provided Precedence Call Waiting is enabled. If the precedence call waiting is not enabled, the caller will block precedence level announcement. SIP stations support MLPP from Communication Manager Release 7.1.

No Hold Conference

An LNCC-active station can initiate a no-hold conference. From Communication Manager Release 8.1, SIP stations support No-Hold Conference feature for J100 series phones.

OPTIM

An off-PBX SIP station supports LNCC.

Personal Station Access/Terminal Translation Initialization

The system saves the LNCC status in the station translation. Therefore, the LNCC status is retained along with the PSA association. SIP stations do not support PSA/TTI.

Priority Call Termination

The LNCC-active station receives a priority call even if the station is busy.

Remote Access

A user cannot use the Remote Access feature to access LNCC.

Send All Calls

If a station has LNCC and SAC activated, the system routes incoming calls to the coverage path of the station.

Transfer

The user of an LNCC-active station can transfer a call only if at least one call appearance is available.

Station Hunting

If an LNCC-active station is busy and if Station Hunting is enabled, the system searches for an idle extension in the station-hunting chain.

Team Button

If an LNCC-active monitored station is busy and the monitoring station makes a call to the monitored station by using the team button, the monitoring station gets a busy tone. However, if an LNCC-active monitoring station is busy, the station can access the calls made to the monitored station by using the team button.

Multi-device Access and Dual Registration

A user can enable the LNCC feature even if the user has more than one endpoint registered to the same extension.

Related links

Limit Number of Concurrent Calls on page 914

Chapter 115: Locally Sourced Announcements and Music

Use the Locally Sourced Announcements and Music feature to access announcement and music audio sources from a local port network or gateway.

Locally sourced audio can help:

- Improve the quality of audio
- Reduce resource usage, such as VoIP resources
- Provide a backup mechanism for announcement and music sources

Detailed description of Locally Sourced Announcements and Music

This feature is available from Communication Manager Release 3.0.

The Locally Sourced Announcement and Music feature differs from the Announcement feature and the Music-on-Hold feature. The Announcement and Music-on-Hold features are single-sourced audio while the Locally Sourced feature is group-sourced audio. Locally Sourced Announcement and Music is based on groups of audio sources. Audio sources are assigned either to an audio group or a music-on-hold group.

Audio groups are made up of multiple sources of the same announcement or music. These audio sources can be located on any or all of the virtual VALs (vVAL) in a gateway, or media server. The VAL, vVAL board, or media server is assigned to an audio group. The audio group is then assigned to an announcement or audio extension as a group sourced location.

Announcement or music recordings are saved as wav file types. Each recording must be saved manually onto the vVAL board, or media server the same way as single-sourced announcements using an FTP program or VAL Manager. Each recording has the same file name within an audio group. The audio group can contain announcements and music.

A music-on-hold group is a collection of externally connected and continuously playing 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.

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.

When an incoming call requires an announcement or music-on-hold, the audio source that is closest to the incoming call trunk plays. An algorithm selects the most local source of audio to play for a call.

The most local source means that it is local to the trunk or user in the same Gateway in the same network region, in the interconnected network region, or is interconnected through an Inter-Gateway Alternate Routing (IGAR). An announcement file extension can be administered for queuing. Under queuing, if the audio source selected to play has no available playback ports, the request to play that audio is held in queue until a port on the source is available. If the queuing option is not administered for the audio file, the search for a local source continues as above.

Accessing audio locally minimizes audio distortion because the audio is located within or close to the same port network or gateway as the caller. Therefore, the Locally Sourced 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.

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.

You can use an announcement or audio source extension with an assigned audio group anywhere that a single sourced announcement or audio source extension can be used. See the Announcements feature or the Music-on-Hold feature for information on single sourced audio.

Note:

For more information on Inter-Gateway Alternate Routing (IGAR), see *Administering Network Connectivity on Avaya Aura® Communication Manager,*.

Locally Sourced Announcements and Music administration

The following tasks are part of the administration process for the Locally Sourced Announcements and Music feature:

- Adding an audio group
- Listing all audio groups
- Changing audio group extensions
- Listing audio group extensions
- Adding a music-on-hold group
- Listing music-on-hold groups
- Changing music-on-hold source type
- Adding music sources to a tenant partition
- Displaying vVAL group descriptions
- Displaying announcement and music system capacities

Related links

Displaying announcement and music system capacities on page 926
Displaying vVAL group descriptions on page 926
Adding an audio group on page 924
Listing all audio groups on page 924
Audio group extension changes on page 925
Listing audio group extensions on page 925
Adding a Music-on-Hold group on page 925
Listing music-on-hold groups on page 925
Changing music-on-hold source type on page 925
Adding music sources to a tenant partition on page 926

Screens for administering Locally Sourced Announcements and Music

Screen name	Purpose	Fields
Audio Groups	List audio group features and announcement extensions.	All
Audio Group	Add, change, or delete audio source locations in an audio group.	All

Table continues…

Screen name	Purpose	Fields
Announcements/Audio Sources	Display and change individual announcements and music-on-hold extensions. Determine properties of audio sources.	All
MOH Group	Add, change, display, delete music-on-hold groups.	All
Music-on-Hold Groups	List all of the music-on-hold groups in the system.	All
Feature-Related System Parameters	Change music-on-hold group source type.	Music/Tone On Hold Type
Tenant	Display the music source for a tenant partition.	Music Source
Music Sources	Add, change, display, delete music sources.	All
Announcement Group Board Usage	Display group identification.	All
System Capacity	Display available extension source combinations capacity.	Extension-Source Combinations

Adding an audio group

Procedure

1. Log in to the Communication Manager CLI.
2. In the command prompt, type **`add audio-group n`**, where n is the group number assigned to an audio group. To assign the next available audio group number in Communication Manager, enter **`add audio-group n`** next.

   Communication Manager displays the Audio Group screen.
3. In the **Group Name** field, enter an identifier name for the group.
4. In the **Audio Source Location** fields, enter the vVAL location designators or the media server for each audio source in the audio group.
5. Press `Enter` to save your changes.

Listing all audio groups

Procedure

1. Enter `list audio-group`.
2. View your settings and exit the screen.

Audio group extension changes

To change audio group extensions for announcements and music, see the Adding/changing/displaying or removing announcement extensions.

Related links

Adding/changing/displaying or removing announcement extensions on page 172

Listing audio group extensions

Procedure

1. Enter `list usage audio-group` *number*, where *number* is the audio group number.
2. View your settings and exit the screen.

Adding a Music-on-Hold group

Procedure

1. Log in to the Communication Manager CLI.
2. In the command prompt, type **`add moh-analog-group n`**, where n is the Music-on-Hold group number.

   Communication Manager displays the MOH Group screen.
3. In the **Group Name** field, enter an identifier name for the Music-on-Hold group.
4. In the **MOH Source Location numbered** fields, enter the Music-on-Hold vVAL source locations.
5. Press `Enter` to save your changes.

Listing music-on-hold groups

Procedure

1. Enter `list moh-analog-group`.
2. View your settings and exit the screen.

Changing music-on-hold source type

Procedure

1. Enter `change system-parameters features`.
2. In the **Music/Tone on Hold** field, type `music`.
3. In the **Type** field, type one of the following values:
   - Type `ext` and the corresponding extension number of the integ-mus announcement/audio source.
   - Type `group` and the corresponding music-on-hold analog group number.

- Type `port` and the corresponding location of the music-on-hold analog/aux-trunk source.

If the **Tenant Partitioning** field on the Optional Features screen is set to y, you cannot administer the **Music/Tone on Hold** field.

If the **Tenant Partitioning** field on the Optional Features screen set to y, you must use the Music Sources screen to assign music to a port.

4. Press `Enter` to save your changes.

Adding music sources to a tenant partition

Procedure

1. Enter `change tenant` *`number`*, where *number* is the partition number.
2. Enter `change music-sources`.
3. In the **Type** field, valid options are music and tone.
4. In the **Source** field, valid options for the music type are:
   - ext - audio source extension for a single or group audio source
   - group - a music-on-hold analog group number
   - port - an analog or auxiliary trunk source location
5. In the **Source** column, after a source type is entered, an entry line appears to the right.

   Type an identifier for the audio source. The identifier is one of the following:
   - audio group extension number,
   - music-on-hold group number, or
   - port location.
6. In the **Description** column, type a description for each music source.
7. Repeat steps 3 to 6 to add up to 100 music sources.
8. Select **Enter** to save your changes.

Displaying vVAL group descriptions

Procedure

Enter `list usage integ-annc-board` *`location`*, where *location* is the 5-character location identification number.

Displaying announcement and music system capacities

About this task

The number of audio groups, audio sources per group, audio files per source and extension-source combinations are limited. Extension-source combinations are the total of the single-sourced announcement extensions and the group-sourced announcement sources that are

assigned in an audio group to each extension. See the *Avaya Aura® Communication Manager System Capacities Table* for the current release to see system capacity limits.

Procedure

Enter `display capacity`.

Interactions for Locally Sourced Announcements and Music

This section provides information about how the Locally Sourced Announcements and Music feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Locally Sourced Announcements and Music in any feature configuration.

Automatic Server Failover Feature

The operation of local audio and music-on-hold sources might not work as intended in cases where the primary server migrates to a backup server. This interruption occurs because the audio sources might be unavailable from the backup server due to physical fragmentation of the network. However, the best available local audio source is still chosen by the backup server.

Multi-Location Dial Plan (MLDP)

Under the Locally Sourced Announcements and Music feature, an audio source is selected based on where the source is located with respect to the user's location. However, under the MLDP feature, the audio source to be used is predefined and based only on the location of the call's ingress point. Also unlike the locally sourced music-on-hold, the MLDP feature does not support music files.

Chapter 116: Location for routing incoming overlap calls

With the Location for routing incoming overlap calls feature, administrators can configure the location to route incoming calls that are mapped to EC500, CSP, and Avaya one-X applications over ISDN-PRI, ISDN-BRI, and H.323 overlap trunks.

Detailed description of Location for routing incoming overlap calls

Before the Location for routing incoming overlap calls feature, incoming off-pbx calls with origination mapping on Communication Manager used the station location when administered to route incoming calls. Origination mapping of off-pbx stations changes the location of origination, which can lead to incorrect manipulation of the called number.

With the Location for routing incoming overlap calls feature, an administrator can configure the location to route incoming calls over ISDN-PRI, ISDN-BRI, and H.323 overlap trunks. The incoming calls are mapped to EC500, CSP, and Avaya one-X applications.

The **Location for routing incoming overlap calls** field is added to the off-pbx Configuration Set screen. This field has two values as follows:

- `trunk`: Communication Manager uses the incoming trunk location to route the call, if you set the **Location for routing incoming overlap calls** field to `trunk`.
- `station-location-if-set`: Communication Manager uses the station location only, if the location is configured on the EC500-mapped station screen.

For more information about the field description, see *Avaya Aura® Communication Manager Screen Reference*The Location for routing incoming overlap calls feature is applicable only to overlap trunks.

The overlap trunk refers to an ISDN trunk group configured for overlap receiving. The **Digit Handling (in/out)** field on the ISDN Trunk Group screen is set to `overlap/overlap` or `overlap/enbloc`.

Note:

As the **Location** field is not configured for DCP stations, an incoming EC500 call mapped to a DCP station always uses the trunk location to route the call.

System requirements for Location for routing incoming overlap calls

Scope and use of incoming trunk location

When you enable the Location for routing incoming overlap calls feature, Communication Manager uses the location of the incoming overlap trunk to manipulate and route the incoming call. For any routing done after the called number is routed, Communication Manager uses the location of the EC500-mapped station.

Note:

The Location for routing incoming overlap calls feature overrides the station location with the trunk location only during the initial routing of the call.

Feature Name Extension processing of incoming calls over overlap trunks

Communication Manager uses the location of the EC500-mapped station after the Feature Name Extension (FNE) is active.

For example, a user dials the FNE to select an idle call appearance from the mobile. After the user selects the call appearance and hears the dial tone, all numbers dialed are processed by using the location of the station and not the location of the incoming trunk.

Screen for administering Location for routing incoming overlap calls

Screen name	Purpose	Field
Configuration Set	To configure the location to route incoming overlap calls.	Location for routing incoming overlap calls

Chapter 117: Loss Plans

Detailed description of Loss Plans

Caution:

The values in the loss plan can significantly affect the quality of service that your users experience. Therefore, to change the loss plan you must thoroughly understand loss plans and your particular configuration. Avaya recommends that you seek technical assistance from Avaya before making any modifications to the loss plan.

Use the 2 Party Loss Plan page of the Location Parameters screen to set the decibel gain or loss levels, between two parties on a call. Each row on this screen is considered a different loss group. You can assign a loss group to a particular phone or trunk by administering a value for the **Loss Group** fields on the Station and Trunk Generation screens. You can use this setting for loss plans for different types of phones or different trunk groups.

With the Tone Loss Plans page on the Location Parameters screen, you can set the tone gain or loss levels (in dB) on a conference call, and the total gain or loss in a conference based on the number of parties.

Note:

The end-to-end total loss for multi-party conference calls that is administered on the Location Parameters screen is not always applied to a specific call. The loss applied to, for example, a 3-party conference call is calculated by adding the fixed pairwise loss for each pair of ports to the value for 2-party loss shown on the Location Parameters screen. If this total is less than the end-to-end total loss value configured for a 3-party conference, calculate the difference, and divide the difference by 2. Add 1 to this figure, and the result is the amount of loss applied to the call.

IP endpoints connected using hairpinning or direct IP-IP are not under the control of the administrable loss plan.

Loss Plans administration

This section describes the prerequisites and the screens for the Attendant Direct Trunk Group Selection feature.

Related links

Guidelines for using loss groups on page 931

Preparing to administer Loss Plans

About this task

- Ensure that the **Digital Loss Plan Modification** field on the Optional Features screen is set to y.

  If the value of this field is n, your system will not support the Loss Plans feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering the Loss Plan feature, or to open a service request.

  To view the Optional Features screen, enter **`display system-parameters customer-options`**.

- Ensure that the **Customize** field on the Location Parameters screen is set to y.

  To view the Location Parameters screen, enter `display location-parameters`.

Guidelines for using loss groups

The following guidelines are provided for using the loss groups:

- Use loss groups 1, 2, 3, 4, 5, and 19 for the following types of stations:
  - 1, 4, and 5 for analog stations
  - 2 for digital stations
  - 3 for BRI stations
  - 19 for IP stations
- Use loss groups 6, 7, and 8 for analog central office (CO) trunks. Analog CO trunks must not use other loss groups.
- Use loss groups 12, 13, and 14 for digital tie trunks.
- Use loss groups 9 and 10 for analog tie trunks.
- Use loss group 15 for tie trunks (analog or digital) where the length of the trunks are less than 100 miles. For example, always select the loss group 15 for tie trunks connecting switches on the same campus.
- Use loss group 11 for digital CO trunks.

Related links

Loss Plans administration on page 930

Screens for administering Loss Plans

Screen name	Purpose	Fields
Optional Features	• Shows whether or not the Loss Plans feature is enabled on your system.	• Digital Loss Plan Modification
Location Parameters	• Customize the Loss Plans feature. • Shows the digital loss group number that is used by the virtual IP tie trunks.	• Customize • Inter-location Loss Group
Station	• Shows the index into the loss plan and the tone plan	• Loss Group
Trunk Group	• Shows the index into the loss plan and the tone plan if the call is carried over an analog or a digital signaling port in the trunk group.	• Analog Loss Group • Digital Loss Group
Personal CO Line Group	• Shows the index into the loss plan and the tone plan if the call is carried over an analog or a digital signaling port in the personal co line group.	• Analog Loss Group • Digital Loss Group

Chapter 118: Loudspeaker Paging

Using the Loudspeaker Paging feature you can connect Communication Manager to loudspeaker systems and users can page from user telephones.

Detailed description of Loudspeaker Paging

You can administer up to nine separate zones, or sets of loudspeakers on Communication Manager. Thus, you can make an announcement to one group or location without disturbing people who do not need to hear the announcement. Auxiliary trunks connect the speakers in each zone to ports on an auxiliary trunk media module.

Types of Loudspeaker Paging

Communication Manager offers two types of loudspeaker paging. You can use each separately, and you can also use both together.

Voice paging

With voice paging, users can make announcements over a loudspeaker system from their phones. You can integrate voice paging and Call Park by enabling Deluxe Paging.

Chime paging

If frequent voice pages are undesirable, you can assign a unique series of chimes, or a chime code to each extension. The chime code assigned to that extension plays over the speakers when that extension is paged.

Chime paging is sometimes called Code Calling Access.

Deluxe paging

With standard voice paging, users page by dialing the Trunk Access Code assigned to the zone they want to page. If users have an active call, the users must manually put the call on hold or park the call before they dial the TAC.

When you enable deluxe paging, users can automatically park an active call when they use the voice paging feature.

Deluxe Paging for users with multiappearance telephones

The following description applies only to systems with deluxe paging. To page and park an active call simultaneously, users with a multiappearance phone press **Transfer**, dial the trunk access code + an extension number where the call will be parked, make the announcement, and press Transfer again. The paged party dials the answer back Feature Access Code + the extension number and is connected directly to the parked call. If the paging user presses **Conference** instead of **Transfer**, they are conferenced with the parked caller and both are connected in a three-way conference with the paged user when that user responds. This is called Meet-Me Conferencing.

If the paging user does not want to park the active call, Deluxe Paging also allows Meet-Me Paging. Paging users can put an active call on hold and make their page, announcing their own extension. When the paged party calls, the paging user can conference the call on hold or transfer it to the paged party.

Deluxe Paging for users with single-line phones

This description only applies to systems with deluxe paging. To page and park an active call simultaneously, users with a single-line phone press **Recall** or flash the switch hook, dial the trunk access code + an extension where the call will be parked, and press **Recall** again. The paging user is conferenced with the parked caller and both parties are connected in a three-way conference with the paged user when he or she responds. In other words, Meet-Me conferencing is standard operation for users with single-line phones. The paged party dials the answer back Feature Access Code + the extension number and is connected directly to the parked call.

If the paging user does not press **Recall** until the loudspeaker paging time-out interval expires, the user hears a confirmation tone, and the active call is automatically parked on their extension. When the paged party answers the call. The paged party is connected to the paging party. The paging party can then transfer the call to the calling party.

Deluxe paging support for branch gateways

Using the deluxe paging support for branch gateways feature you can use the deluxe paging with analog media modules (MM711 and MM714).

Deluxe paging for analog trunks

To use the deluxe paging feature with analog trunks, the analog trunk port must be connected to an analog line port. The analog line ports are administered as passive signaling stations. Analog trunks need a line-end termination to remain in-service and close the circuit. Stations administered as passive signaling stations act as line-end terminations for analog loop start trunk ports.

Chime paging

To page a user, dial the TAC for a zone, and then dial the extension of the user. The system matches the extension dialed to its assigned code and plays the code over loudspeakers. If users have an active call when they start to page, the call is automatically parked on the extension dialed in the page. Paged parties may retrieve the parked call normally.

Auxiliary paging systems

Communication Manager requires a separate port for each paging zone, and supports a maximum of nine zones. If you have more than nine zones or do not want to allot that many ports for paging, Avaya can provide auxiliary paging systems. These systems can support many zones from 1 port. They can also provide additional capabilities such as two-way communication through the loudspeaker system. In this case, the person paged can speak directly to the pager over the loudspeaker.

Restrictions on loudspeaker paging

These restrictions apply to both voice, deluxe voice, and chime paging:

- A paging call cannot be placed on hold, included in a conference call, or transferred. Also, ringback queuing does not work with loudspeaker paging calls either.
- Users with any of the following restrictions cannot page:
  - Controlled restriction
  - Manual originating line service
  - Origination restriction
  - Miscellaneous trunk restriction
- A user with a single-line telephone does not hear a call-waiting tone if the user gets a call while paging.
- Listed Directory Number (LDN) and Direct Inward Dialing (DID) calls cannot access the paging system. However, attendants can park incoming calls and page.
- Remote users (such as remote access users and tie-trunk users) who are paging cannot use # to park calls on their own extensions.

Loudspeaker Paging administration

The following tasks are part of the administration process for the Loudspeaker Paging feature:

- Setting up Voice Paging over loudspeakers
- Setting up Chime Paging over Loudspeakers
- Assigning a chime page code to an individual extension

Related links

Assigning a chime page code to an individual extension on page 939
Setting up Chime Paging over Loudspeakers on page 937
Setting up Voice Paging over loudspeakers on page 937

Preparing to administer Loudspeaker Paging

Procedure

1. The server that runs Communication Manager must have one or more auxiliary trunk media modules with enough available ports to support the number of paging zones that you define.

   Each paging zone requires one port.

2. To set up deluxe paging, view the Feature-Related System Parameters screen.

   Ensure that the **Deluxe Paging and Call Park Timeout to Originator** field is set to y.

   To view the Feature-Related System Parameters screen, enter `change system-parameters features`.

Screens for administering Loudspeaker Paging

Screen name	Purpose	Fields
Feature-Related System Parameters	Set up deluxe paging.	Deluxe Paging and Call Park Timeout to Originator
Station	Set up Passive Signaling Station for deluxe paging.	Passive Signaling Station
Loudspeaker Paging	Assign Analog Trunk Port to support deluxe paging for branch gateways.	Port
	Set up voice paging over loudspeakers.	• Voice Paging Timeout • Port • Voice Paging - COR • Voice Paging - TAC • Location
	Set up chime paging over loudspeakers	• Code Calling Playing Cycles • Port • Voice Paging - TAC • Voice Paging - COR • Location • Code Calling - TAC
Code Calling Ids	Set up chime paging over loudspeakers	• Ext • Id

Setting up Voice Paging over loudspeakers

Procedure

1. Enter `change paging loudspeaker`.
2. In the **Voice Paging Timeout** field, type the maximum number of seconds that a page can last.
3. In the **Port** field for Zone 1, type the port number that is assigned to the auxiliary media module to this zone.
4. In the **Voice Paging - TAC** field, type the value for Trunk Access Code (TAC) that users dial to page this zone.
5. In the **Voice Paging - COR** field, type the class of restriction (COR) for this zone.

   You can assign different CORs to different zones.
6. In the **Location** field on the Zone 1 row, type a descriptive name for the zone.

   Use this name to help you remember the corresponding physical location.
7. Repeat steps 4 through 6 for each zone.
8. In the **ALL** row of the **Voice Paging- TAC** field, type the value for Trunk Access Code (TAC) that users dial to page all zones.
9. In the **All** row of the **Voice Paging - COR** field, type the class of restriction (COR) for all zones.

   When you complete this row, you allow users to page all zones at once. You do not have to assign a port to this row.
10. Press `Enter` to save your changes.

    You can integrate loudspeaker voice paging and call parking. This is called “deluxe paging.” You enable deluxe paging by entering y in the **Deluxe Paging and Call Park Timeout to Originator** field on the Feature-Related System Parameters screen. To allow paged users the full benefit of deluxe paging, you must enter a code in the **Answer Back Access Code** field on the Feature Access Code (FAC) screen if you have not done so already. Paged users dial the FAC, plus an extension to retrieve calls parked by deluxe paging.

    Note:

    To set up paging on an H.248 gateway, connect the paging system to a port on an MM711 and administer the port as an analog station on the Station screen. No entries on the Loudspeaker Paging screen are required.

Setting up Chime Paging over Loudspeakers

Procedure

1. Enter `change paging loudspeaker`.

The system displays the Loudspeaker Paging screen (the figure on page 938).

In this example, you set up chime paging for a clothing store with three zones. You allow users to page all three zones at once, and you assign a Class of Restriction (COR) of 1 to all zones.

```
                            LOUDSPEAKER PAGING

                                    CDR? y
              Voice Paging Timeout (sec):
             Code Calling Playing Cycles: 2

PAGING PORT ASSIGNMENTS
                   Voice Paging      Code Calling
 Zone   Port        TAC   COR  TN     TAC   COR  TN     Location:
   1:   01A0301                1      80     1   1      Men's Department
   2:   01A0302                1      81     1   1      Women's Department
   3:   01A0303                1      82     1   1      Children's
   4:                          1                 1
   5:                          1                 1
   6:                          1                 1
   7:                          1                 1
   8:                          1                 1
   9:                          1                 1
 ALL:                          1      89     1   1
```

Figure 20: Loudspeaker Paging screen

2. In the **Code Calling Playing Cycles** field, type the number of times that a chime code plays when someone places a page.
3. In the **Port** field for Zone 1, type the port number of the auxiliary trunk media module that is assigned to this zone.

   In this example, the port number is 01A0301.
4. In the **Code Calling - TAC** field, type the Trunk Access Code (TAC) users dial to page this zone.

   You cannot assign the same trunk access code to more than one zone.

   In this example, the trunk access code is 80.
5. In the **Code Calling - COR** field, type the COR number that is assigned to this zone. You can assign different classes of restriction to different zones

   In this example, the COR is 1.
6. In the Zone 1 row of the **Location** field, type a descriptive name for the zone.

   Use this name to help you remember the corresponding physical location.

   In this example, the location is Men's Department.
7. Repeat steps 4 through 6 for zones 2 and 3.

8. In the **ALL** row of the **Code Calling - TAC** field, type `89` and `1` in the **Code Calling - COR** field.

   When you complete 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 a chime page code to an individual extension

Procedure

1. Enter `change paging code-calling-ids`
2. In the **Ext** field, type the first extension for Id 111.
3. To assign chime codes to the remaining extensions, type an extension number on the line following each code Id.

   You can assign a different chime code to as many as 125 extensions.

4. Press `Enter` to save your changes.

Setting up Passive Signaling Station for deluxe paging

Procedure

1. Enter `add station` *n*, where *n* is the extension of the station.
2. In the **Type** field, type the model of analog station, such as 2500.
3. Set the **Passive Signaling Station** field to y.
4. Press **Enter** to save your changes.

Assigning an Analog Trunk Port

Procedure

1. Enter `change paging loudspeaker`.
2. In the **Port** field, enter the port number of the analog trunk media module.
3. Press **Enter** to save your changes.

Interactions for Loudspeaker Paging

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

Bridged Call Appearance

If a parked call includes a shared terminating extension group, a shared Personal Central Office Line (PCOL), or a redirected call with a temporary bridged appearance, the maximum number of off-hook parties on the call is five, instead of six. The sixth position is reserved for the answer-back call.

Call Coverage

If a coverage call is parked by deluxe paging, the temporary bridged appearance at the principal extension is maintained as long as the covering user remains off-hook or places the call on hold.

Call Park

If a call is parked by deluxe paging and the time-out interval expires, the call usually returns to the paging user. However, with remote access and tie trunk access, the call returns to the attendant. If unanswered, the call follows the coverage path of the paging user.

Call Pickup

If you use call pickup or directed call pickup to answer a call and then park it by deluxe paging, a temporary bridged appearance at the principal extension is maintained if you remain off-hook or place the call on hold.

Conference -Attendant and Terminal

Paging calls cannot be conferenced.

Data Call Setup

If the **Data** button has been pressed for modem pooling, access to paging is denied.

Data Privacy

If a call has Data Privacy activated and you park it by deluxe paging, Data Privacy for that call is automatically deactivated.

Hunt Groups

If a hunt-group member parks a call using deluxe paging, the call is parked on the member’s own extension, not the hunt-group extension. You cannot park calls on a group extension by dialing the extension as a call-park destination.

Night Service

If a night-station user parks a Night Service call with deluxe paging, the call is parked on the night station’s primary extension.

Personal Central Office Line (PCOL)

If a PCOL call is parked by deluxe paging, the temporary bridged appearance of the call is maintained at the PCOL extension until the call is disconnected.

Terminating Extension Group (TEG)

If a TEG member parks a call using deluxe paging, the call is parked on the member’s extension, not the group extension. You cannot park calls on a group extension by dialing the extension as a call-park destination.

Transfer

Paging calls can’t be transferred.

Interactions for Chime Paging

The following interactions are specifically for chime paging:

Abbreviated Dialing

Don’t use special characters in abbreviated dialing lists used with chime paging.

Conference - Attendant

A call cannot be conference while the attendant is accessing paging equipment. The attendant can, however, release the call after paging the called party.

Conference - Terminal

A call cannot be conferenced while the user is accessing paging equipment.

Transfer

A call cannot be transferred while the attendant is accessing paging equipment.

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.

Chapter 119: Malicious Call Trace

Use the Malicious Call Trace (MCT) feature to track malicious calls. Both users and attendants can track malicious calls, and display information that identifies the source of the call. The user or attendant can share the information with personnel on a tandemed server. The personnel on the tandemed server can continue to trace the call. MCT also supports a voice recorder that records the malicious call.

Detailed description of Malicious Call Trace

Malicious Call Trace (MCT) has three distinct phases:

- Activation
- Control
- Deactivation

Malicious Call Trace Activation

A user or an attendant can use either a feature button (mct-act) or a Feature Access Code (FAC) to activate MCT. Either the recipient of the call, or another user or attendant, can activate MCT.

Malicious Call Trace Control

When a user activates the **mct-act** button, the system notifies the potential MCT controllers. A potential MCT controller is a station or an attendant that has an **mct-contr** button.

Note:

The mct-contr button can only be administered on H.323 or DCP stations or attendants. This functionality is not SIP compatible. If no mct-controller is administered, then the SNMP trap is generated to record the MCT activation.

To notify the potential MCT controllers, the system:

- Generates an alert tone.
- Flashes the indicator of the **mct-contr** button.

The user who presses the **mct-contr** button first becomes the MCT controller of the call. The system stops alerting other potential MCT controllers.

- The called number
- The activating number
- The status of the call
- The details of the other parties on the call

The user of the MCT controller must continue to press the **mct-contr** button to see the entire MCT information.

Depending on the origin of the call, the system displays:

- The calling number if the call originates inside the system or on the same node within a Distributed Communications System (DCS) network.
- The calling number if the call originates outside the system and an Integrated Services Digital Network (ISDN) or SIP calling number identification is available on the incoming trunk.
- The location of the incoming trunk for all other calls. In this case, the user must call the connecting server to get more information about the malicious call.

Malicious Call Trace Deactivation

The MCT controller dials the FAC for MCT deactivation to deactivate MCT. Deactivation frees any blocked resources that were involved in the trace. When all parties hang up, the system disconnects the MCT voice recorder.

If the controller list configured by the command **`change mct-group-extensions`** is empty which means that no mct-controller is administered, then MCT is deactivated when all parties hang up. An SNMP trap is generated to record the activation of MCT. This SNMP trap is critical while configuring with all SIP endpoints, as the endpoint cannot be the MCT Controller.

MCT voice recorder

The MCT voice recorder can be any standard audio cassette player that the Avaya Auxiliary Trunk board can control.

To record a call, manually place the MCT voice recorder in Record MCT mode, and then activate MCT. The activated feature uses the control signal interface of the auxiliary trunk that is connected to the MCT voice recorder to apply power to the recorder.

Note that the system temporarily removes any Bridging, Conference, or Intrusion tones during the time that the MCT voice recorder is connected.

Malicious Call Trace administration

The following tasks are part of the administration process for the Malicious Call Trace feature:

- Defining Malicious Call Trace on your system
- Assigning a feature button to control Malicious Call Trace
- Assigning a Malicious Call Trace feature button for an attendant
- Assigning a Malicious Call Trace feature button for a user
- Administering Malicious Call Trace for ISDN notification

Note:

From Communication Manager Release 7.1.3 onwards, Malicious Call Trace notifications over SIP trunks are also supported.

Related links

Administering Malicious Call Trace for ISDN notification on page 947
Assigning an MCT feature button for a user on page 947
Assigning an MCT feature button for an attendant on page 946
Assigning feature button to control MCT on page 946
Defining Malicious Call Trace on your system on page 945

Preparing to administer Malicious Call Trace

Procedure

1. View the Optional Features screen, and ensure that the **Malicious Call Trace** field is set to y.

   If the **Malicious Call Trace** field is set to n, your system does not support the MCT feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering the Malicious Call Trace feature, or to open a service request.

   To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

2. Ensure that a Class of Restriction (COR) that enables your users to use the MCT feature exists on your system.

   The MCT feature requires a COR with the **Access to MCT** field set to y.

   For information about COR administration, see the Class of Restriction feature description.

3. Ensure that Feature Access Codes (FACs) to activate and deactivate the MCT feature exist on your system.

   The MCT feature requires the following FACs:

   - Malicious Call Trace Activation

- Malicious Call Trace Deactivation

For information about FAC administration, see the “Feature Access Code (FAC)” feature description.

Related links

Class of Restriction on page 561

Screens for administering Malicious Call Trace

Screen name	Purpose	Fields
Attendant Console	Assign feature buttons for MCT activation and control.	• mct-act • mct-contr
Class of Restriction	Define a Class of Restriction (COR) that allows MCT.	• Access to MCT?
FAC	Specify the Feature Access Codes (FACs) for MCT activation and deactivation.	• Malicious Call Trace Activation • Malicious Call Trace Deactivation
Malicious Call Trace Control Extensions	Specify the extensions that can use the mct-contr feature button.	All
ISDN-BRI Trunk Media Module	Administer ISDN MCT notification for an ISDN trunk group.	• Cntry/Peer Protocol • Interface
DS1 Media Module	Administer ISDN MCT notification for an DS1media module.	• Country Protocol • Protocol Version • Peer Protocol
Station	Assign an mct-act and an mct-contr feature button for a user.	Any available button field in the **Button Assignments** area
Feature-Related System Parameters	Specify that an MCT controller hears a tone when the MCT voice recorder is active.	Apply MCT Warning Tone?
	Assign the trunk group for MCT voice recorders.	MCT Voice Recorder Trunk Group
	Specify the wait time or a release message.	Delay Sending Release (seconds)

Defining Malicious Call Trace on your system

Procedure

1. Enter `change system-parameters features`.
2. Click **Next** until you see the **Apply MCT Warning Tone?** field.

3. In the **Apply MCT Warning Tone?** field, perform one of the following actions:
   - If you want the system to generate a tone at the telephone that controls MCT when the MCT voice recorder is active, type `y`.
   - If you do not want the system to generate a tone at the telephone that controls MCT when the MCT voice recorder is active, type `n`.
4. In the **MCT Voice Recorder Trunk Group** field, type the trunk group for MCT voice recorders.
   - For DEFINITY R, CSI, and S1, valid entries are a number from 1 to 666.
   - For the IP-PNC servers, valid entries are a number from 1 to 2000.
5. In the **Delay Sending Release (seconds)** field, type the number of seconds that the server waits to send an ISDN release message, after the server receives an ISDN disconnect message.
   - Valid entries are 0, 10, 20, or 30.

     The system displays this field only if the **Malicious Call Trace?** field on the Optional Features screen is set to y.
6. Select `Enter` to save your changes.

Assigning feature button to control MCT

Procedure

1. Enter `change mct-group-extensions`.
2. In any numbered field, type the extension of a user or an attendant console that you want to have an mct-contr feature button.

   For every extension and attendant console that you administer, you must assign an mct-contr feature button. You assign these buttons for the attendant on the Attendant Console screen, and for the user on the Station screen.
3. Select **Enter** to save your changes.

Assigning an MCT feature button for an attendant

Procedure

1. Enter `change attendant` *n*, where *n* is the number of the attendant to which you want to assign an MCT feature button.
2. Click **Next** until you see the **Feature Button Assignments** area.
3. Type `mct-act` next to the button number that you want the attendant to use to activate MCT.
4. Type `mct-contr` next to the button number that you want the attendant to use to establish control of the malicious call, and to display information about the call.
5. Press `Enter` to save your changes.

Assigning an MCT feature button for a user

Procedure

1. Enter `change station n`, where *n* is the number of the station to which you want to assign an MCT feature button.
2. Click **Next** until you see the **Button Assignments** area.
3. Type `mct-act` next to the button number that you want the user to use to activate MCT.
4. Type `mct-contr` next to the button number that you want the user to use to establish control of the malicious call, and display information about the call.
5. Press `Enter` to save your changes.

Administering Malicious Call Trace for ISDN notification

About this task

SIP trunks do not need any special configuration for Communication Manager to send the Malicious Call Trace notification

Use Steps 1 to 5 for ISDN-PRI connections and Steps 6 to 10 for ISDN-BRI trunk connections, as appropriate for your network. Communication Manager does not send MCT notification over ISDN/H.323 trunks.

Procedure

1. In the Communication Manager CLI, enter `add ds1 n`, where *n* is the number of the DS1 media module that you want to add.
2. In the **Country Protocol** field, do one of the following:
   - If the DS1 is connected to a public network in Australia, type `2`.
   - If the DS1 is connected to a public network that supports the ETSI Malicious Call Trace Identification (MCID) service according to EN 300 130, type `etsi`.
   - If the DS1 is connected to a private network of servers that run Communication Manager, type `1`.
3. In the **Peer Protocol** field, type `q-sig`, if the DS1 is connected to a private network of servers that run Communication Manager.

   The system displays the **Peer Protocol** field when the:

   - **Signaling Mode** field is set to isdn-pri.
   - **Connect** field is set to pbx.
   - **Interface** field is set to either peer-master or peer-slave.
4. To administer other fields on the DS1 Media Module screen, see *Administering Avaya Aura® Communication Manager*.
5. Press `Enter` to save your changes.

6. Enter `change bri-trunk-board`.
7. In the **Cntry/Peer Protocol** field, type one of the following: * `2` if the ISDN-BRI media module is connected to a public network in Australia.

   * `etsi` if the ISDN-BRI media module is connected to a public network that supports the ETSI Malicious Call Trace Identification (MCID) service according to EN 300 130.
8. In the **Interface** field, type either `peer-master` or `peer-slave`, if the ISDN-BRI media module is connected to a private network of servers that run Communication Manager.
9. To administer other fields on the ISDN-BRI Trunk Media Module screen, see *Administering Avaya Aura® Communication Manager*.
10. Press `Enter` to save your changes.

Note:

You must set the **Supplementary Service Protocol** field on the ISDN Trunk Group screen to a for Australia and c for ETSI.

End-user procedures for Malicious Call Trace

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Activating MCT with a feature button when you receive a malicious call

Procedure

Press the **mct-act** feature button.

Activating MCT with a FAC when you are active on a call

Procedure

1. Place the call on hold, transfer, or conference.
2. Get a second call appearance.
3. Dial the FAC to activate MCT.
4. When you hear the dial tone, perform one of the following actions:
   - Dial your extension.
   - Press the pound key (#).

   If you press the pound key`#`, the system traces the call at your extension.

5. Wait 10 seconds to hear the confirmation tone that the system generates.

Activating MCT with a FAC when you are not active on a call

Procedure

1. Dial the FAC to activate MCT.
2. Perform one of the following actions:
   - Dial the extension number that received the malicious call.
   - Dial a trunk access code (TAC) and the subsequent member number.

Requesting that an MCT controller on a tandemed server continue the trace

Procedure

1. Contact the controller on the tandemed server.
2. Provide the trunk port ID that you want the controller on the tandemed server to trace
3. The controller on the tandemed server:
   a. Activates MCT
   b. Presses the star key (*)
   c. Dials the trunk port ID

      Dial letters A through E of the port ID as the numbers 1 through 5. For example, to dial the trunk port ID 01C0401, press `0130401`.

Displaying MCT information

Procedure

1. Press the **mct-contr** button.
2. Continue to press the button to display all the information that is available about the malicious call.

Deactivating MCT

Procedure

The MCT controller dials the FAC that deactivates MCT.

The system generates confirmation tone, extinguishes all lamps that are related to the MCT call, and disconnects the MCT voice recorder, if a voice recorded was used on the call.

Reports for Malicious Call Trace

The following reports provide information about the Malicious Call Trace (MCT) feature:

- The MCT History report provides information about an MCT incident. This information includes the date and time, the controller and the recorder, the parties who were involved on the call, and whether or not the public network was notified about the call.

For detailed information on these reports and the associated commands, see *Avaya Aura® Communication Manager Reports*.

Considerations for Malicious Call Trace

This section provides information about how the Malicious Call Trace feature functions in certain circumstances. Use this information to ensure that you receive the maximum benefits of Malicious Call Trace under all conditions:

- If the originator of the call hangs up, the system discontinues the feature. However, if the recipient of the call hangs up, the system does not discontinue Malicious Call Trace.

  Note:

  When the recipient of the call is a DCP or H.323 station, you cannot hang up the call until the MCT Controller deactivates MCT. However, when recipient of the call is a SIP station, you can hang up the call without the MCT Controller deactivating the MCT.

- Except for Emergency Access to the Attendant, features that usually display information do not display information on the telephone of the Malicious Call Trace controller, when Malicious Call Trace is activated. Except for the display of information, these features function normally until Malicious Call Trace is deactivated.
- Use an mct-act button rather than the Feature Access Code (FAC) to activate Malicious Call Trace because the FAC requires extra time.
- Visually Impaired Attendant Service (VIAS) provides spoken display information for Malicious Call Trace activation, but not for Malicious Call Trace control.
- Malicious Call Trace information on an active malicious call is lost if a server fails while Malicious Call Trace is activated.
- When you request help from a controller on a server in tandem, the following might occur:
  - The malicious caller might hear a warning tone as a result of the intrusion.
  - You can lose continuity on the trace if the person who activates Malicious Call Trace on the server in tandem is not the Malicious Call Trace controller.
- If a malicious call comes in on a non-ISDN trunk, the controller must have the telephone number for the connecting server and a cross-reference of system-trunk port numbers. The controller might also need the DS1 channel number.

- Only H.323, DCP stations, and attendants can be an MCT Contoller. The **mct-contr** button is not supported on any SIP endpoints.

Differences between Button state and Multiple invocation are as follows:

	Button state	Multiple invocation
H.323/DCP phone	The **mct-act** button lights as soon as you press the button, and it stays lit until an MCT Controller deactivates MCT.	You can press the **mct-act** button again and invoke MCT a second time, even if your first invocation has not been deactivated.
SIP phone	The **mct-act** button stays dark when you press the button, and it does not light until an MCT Controller presses the **mct-control** button.	You cannot press the **mct-act** button a second time. If you do, you get a denial tone.

Interactions for Malicious Call Trace

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

Bridged Call Appearance

The system records the primary extension as the Malicious Call Trace recipient when the feature is activated at a bridged call appearance, or for a bridged call appearance.

Conference

A user can use conferencing to place a malicious caller on hold. The user can start a conference, dial the Feature Access Code (FAC) that activates Malicious Call Trace, and then stop conferencing and return to the call appearance of the malicious caller.

The feature can also be activated for a member of a conference. The Malicious Call Trace activation is unaffected by the number of parties on the conference.

Centralized Attendant Service

The activation, control, and deactivation of Malicious Call Trace for a call must occur on the same server.

Distributed Communications System

If a telephone in a Distributed Communications System network is involved in a malicious call, the system records and displays the extension with the Malicious Call Trace information. Malicious Call Trace notification passes over ISDN-PRI DCS trunks, but the activation, control, and deactivation of Malicious Call Trace must be performed by telephones that are on the same Distributed Communications System node.

Emergency Access to the Attendant

Usually, during MCT-Control, no other feature can access the display of the controlling telephone. However, Malicious Call Trace gives up control of the display until an Emergency Access call is completed.

Make-Busy/Position-Busy/Send All Calls

The software attempts to activate Make-Busy or Position-Busy for telephones or consoles that activate MCT-Control. If a user has a **Send All Calls (SAC)** button administered but inactive for the primary extension on the phone, SAC is activated when the user activates MCT-Control. When the user deactivates Malicious Call Trace, SAC remains active until the user deactivates SAC.

Music-On-Hold

If an agent places a malicious call that is being recorded on hold, and the call goes to music-on-hold, the music-on-hold port and the MCT voice recorder port can get locked too long In this case, the Malicious Call Trace voice recorder continues to record the music-on-hold and is unavailable to record subsequent malicious calls. You must busy out or release the Malicious Call Trace voice recorder port to drop the connection.

Priority Calling

The system denies a priority call to an Malicious Call Trace recipient.

QSIG Global Networking

Malicious Call Trace notification passes over tandem, tie, access, and DMI-BOS ISDN QSIG trunk groups. The name and number ID of the QSIG supplementary services provide the name and telephone number of a malicious caller.

SIP Trunks

Malicious Call Trace notification passes over SIP trunk groups through Session Manager to a Session Border Controller. The Session Border Controller can adapt the Malicious Call Trace notification to the format required by the SIP service provider.

Transfer

If a user transfers a malicious call, the Malicious Call Trace information that the system displays on the telephone of the Malicious Call Trace controller identifies the party that is transferred as the Malicious Call Trace recipient.

Trunk Access Code (TAC)

To activate Malicious Call Trace for a TAC, a user must have an mct-contr feature button administered. The user hears a dial tone and enters the trunk-member number for the trunk group that the TAC identified. The user then becomes the Malicious Call Trace controller for a call that involves the identified trunk member. This TAC operation is useful when users must trace a call that tandemed through their server or toggle to terminate on another server or switch.

Trunk groups

If a personal central office line is involved in a malicious call trace, the software might hold up the trunk until the Malicious Call Trace is deactivated.

Malicious Call notification using Crisis Alert button

From Release 10.1.0.2 onwards, Communication Manager enables users to press the mct-act button after recognizing that the currently active call is malicious. All SIP users with a **Crisis Alert** button are notified about the malicious call provided the Communication Manager has **Notification using Crisis Alert** field enabled on the Feature-Related System Parameters screen.

- If **Notification using Crisis Alert** field is enabled, all SIP users with a Crisis Alert button are notified about the malicious call. During this time, SIP users with a Crisis Alert button are not notified when an emergency call is placed. Consequently, SIP stations do not need to be present in the **mct-group-extensions** table.
- If **Notification using Crisis Alert** is disabled, only MCT Controllers such as DCP and H.323 stations with an mct-control button are notified. Here, the mct controller button and extension are present in the **display mct-group-extensions** table.

Note:

Crisis alert functionality can be disabled for emergency calls. To enable crisis alert for emergency calls, disable the **Notification using Crisis Alert** field on the Feature-Related System Parameters screen, page 5.

The following details are displayed on the user's endpoint with a crisis alert button when mct-act is activated:

- Extension of the user that invoked MCT
- Name of the user that invoked MCT, prefixed with "MCTA-".
- MCT invocation date
- MCT invocation time

Chapter 120: Manual Message Waiting

Use the Manual Message Waiting feature to cause the **Manual Message Waiting** button lamp at another user telephone to light.

Detailed description of Manual Message Waiting

A user presses the designated button to light the **Manual Message Waiting** button lamp at the telephone of another user telephone. Both the telephones must be multiappearance telephones. To turn the lamp off, either telephone user can press the **Manual Message Waiting** button.

You can administer Manual Message Waiting for pairs of telephones only. These telephones might be used by two people who share the same job function and often take calls for one another. The Manual Message Waiting feature is also useful in situations where one person usually answers calls for a second person, such as an administrative assistant might do for a manager. The administrative assistant can press a **Manual Message Waiting** button to signal the manager that a call must be answered. The manager can answer the call or press a **Manual Message Waiting** button to indicate that the administrative assistant should handle the call

Manual Message Waiting administration

The following task is part of the administration process for the Manual Message Waiting feature:

- Assigning The Manual Message Waiting feature button

Related links

[Assigning the Manual Message Waiting feature button](#) on page 955

Screens for administering Manual Message Waiting

Screen name	Purpose	Fields
Station (multiappearance)	Assign the man-msg-wt feature button for a user.	Any available button field in the **Button Assignments** area

Assigning the Manual Message Waiting feature button

Procedure

1. Enter `change station n`, where *n* is the extension of the user to whom you want to assign a Manual Message Waiting feature button.
2. Click **Next** until you see the **Button Assignments** area.
3. In the **Button Assignments** area, type `man-msg-wt` next to the button that you want the user to use for Manual Message Waiting.
4. Press `Enter` to save your changes.

Chapter 121: Manual Signaling

Use the Manual Signaling feature to signal another user.

Detailed description of Manual Signaling

With the manual signaling feature, one user can signal another user. When a user presses the manual signaling button, the other user hears a 2-second ring. The status lamp of the user who presses the button lights for two seconds.

If the telephone of the intended recipient of the signal is already alerting, the system:

- Does not generate the 2-second ring
- Causes the manual signaling button lamp of the user who presses the button to flicker briefly

Manual Signaling administration

The following task is part of the administration process for the Manual Signaling feature:

- Assigning a manual signaling button for a multiple-call appearance telephone user

Related links

Assigning a manual signaling button for a multiple-call appearance telephone user on page 957

Screens for administering Manual Signaling

Screen name	Purpose	Fields
Station (multiappearance)	Assign a **signal** button to the telephone of a user, and specify the extension that rings when the user presses the button.	Any available button field in the **Button Assignments** area

Assigning a manual signaling button for a multiple-call appearance telephone user

Procedure

1. Enter `change station n`, where *n* is the telephone number of the extension to which you want to assign a manual signaling button.
2. Click **Next** until you see the **Button Assignments** area.
3. Type `signal` next to the number of the button that you want the user to use for manual signaling.

   When you type `signal` next to the button number, the system displays an **Ext:** field.
4. Type the extension of the recipient of the signal in the **Ext:** field.
5. Press `Enter` to save your changes.

End-user procedures for Manual Signaling

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. End users can press the manual signal button to access Manual Signaling.

Interactions for Manual Signaling

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

Data Modules

If you administer a manual signaling button for a data module, the system denies any attempt to activate the button.

Vector Directory Number (VDN)

A manual signaling button cannot point to a VDN.

Chapter 122: Media encryption using AES-256

From Communication Manager Release 7.0, the AES encryption option now includes AES-256 cipher suite. AES-256 applies to voice media streams and video media streams for the IP network region that governs the IP codec set. The feature also introduces a mechanism to define the encrypted SRTCP policy for calls governed by the IP network region.

Related links

Detailed description on page 958
Screen for administering Media encryption using AES-256 on page 959
Administering Media encryption using AES-256 on page 959

Detailed description

Advanced Encryption Standard (AES) is a widely used specification for data encryption. The AES standards describe a symmetric key algorithm. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Avaya Aura® Release 6.3 Feature Pack 4 supports AES-256 as part of TLS support over control channels. From Release 7.0, the AES-256 support extends to secure media streams.

To enable Media encryption feature, two more encryption choices are available for the **Media encryption** field on the ip-codec-set SAT screen. The choices are as follows:

- srtp-aescm256-hmac80
- srtp-aescm256-hmac32

Before Release 7.0, the **Media Encryption** field supported only three profiles. Release 7.0 onwards, the field supports five profiles.

You can add the following profiles to Media Encryption:

1. 10-srtp-aescm256-hmac80
2. 11-srtp-aescm256-hmac32
3. 1-srtp-aescm128-hmac80
4. 2-srtp-aescm128-hmac32
5. None

The AES-256 feature is supported on G450 Branch Gateway, G430 Branch Gateway, and Avaya Aura® Media Server (MS).

When you enable the AES-256 feature, Communication Manager determines the capability exchange with G450 Branch Gateway, G430 Branch Gateway, or Avaya Aura® Media Server (MS) and the 96x1 SIP phone. To establish call connections for media services encrypted with AES-256, an SDP media descriptor exchange occurs. During this exchange, Communication Manager functions as a back-to-back user agent. In this role, Communication Manager supports policy management over the SIP endpoints when the endpoints exercise capability negotiation.

Related links

Media encryption using AES-256 on page 958

Screen for administering Media encryption using AES-256

Screen name	Purpose	Fields
Ip-codec-set	To select a type of media encryption.	Media encryption

Related links

Media encryption using AES-256 on page 958

Administering Media encryption using AES-256

Before you begin

Ensure that the **Media Encryption Over IP?** field on the system-parameters customer-options screen is set to `y`.

Procedure

1. On the SAT screen, type `change ip-codec-set n`, where n is the number of the codec set that you want to change.
2. In the **Media encryption** field, type one of the following values:
   - To use encrypted and authenticated RTP with an 80-bit authentication tag, type `10-srtp-aescm256-hmac80`.
   - To use encrypted and authenticated RTP with a 32-bit authentication tag, type `11-srtp-aescm256-hmac32`.
3. Save and exit.

Related links

Media encryption using AES-256 on page 958

Chapter 123: Meet-me Conference

Use the Meet-me Conference feature to set up a dial-in conference of up to six parties. The Meet-me Conference feature uses Call Vectoring to process the setup of the conference call.

Note:

For 12 parties to participate in a Meet-me Conference, you must enable the **12–party Conferences** field in the Feature-Related System-Parameters screen.

Detailed description of Meet-me Conference

With the Meet-me Conference feature, a station user can host a dial-in conference of up to six parties. However, if the **12–party Conferences** field is enabled in the Feature-Related System Parameters screen, 12 parties can participate in a Meet-me Conference call. You can set up the Meet-me Conference extension to require an access code. If you administer an access code, all parties must correctly enter the access code to join the conference. If the extension is one of your Direct Inward Dialing (DID) numbers, any internal or remote access users, or external parties, can dial the Meet-me Conference extension.

When a caller dials into a Meet-me Conference, the system plays an announcement. The announcement tells the caller to enter an access code, if an access code is required. If the caller enters the correct access code, the caller is added to the conference. If no other parties are on the conference, an announcement tells the caller that he is the first caller to join the conference. If other parties are already on the call, an announcement tells the caller that he is joining a conference that is already in progress. All parties who are already on the conference and the newly added party hear an entry tone. When a party drops out of the conference, the remaining parties hear an exit tone.

Meet-me Conference administration

The following tasks are part of the administration process for the Meet-me Conference feature:

- Creating or changing a Meet-me Conference vector
- Creating a Meet-me Conference VDN

Related links

Creating a Meet-me Conference VDN on page 965
Creating or changing a Meet-me Conference vector on page 962

Preparing to administer Meet-me Conference

Procedure

1. On the Optional Features screen, ensure that the **G3 Version** field is set to V11 or later.

   If you do not set the **G3 Version** field to V11 or later, your system does not support the Meet-me Conference feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering the Meet-me Conference feature, or to open a service request.

   To view the Optional Features screen, enter `display system-parameters customer-options`.

2. On the Optional Features screen, click `Next` until you see the **Enhanced Conferencing** field.

   Ensure that this field is set to y. If the **Enhanced Conferencing** field is set to n, your system is not enabled for the Meet-me Conference feature. Contact your Avaya representative before you continue with this procedure.

Screens for administering Meet-me Conference

Screen Name	Purpose	Fields
Optional Features	Ensure that you have Communication Manager version 1.3 (V11) or greater.	G3 Version
	Ensure that Enhanced Conferencing is enabled.	Enhanced Conferencing
Call Vector	Create a Meet-me Conference vector.	All
Vector Directory Number	Set up a VDN for Meet-me Conference.	• Extension • Name • Vector Number • Meet-me Conferencing • Conference Access Code • Conference Controller
Meet-me Vector Directory Number	View a list of existing Meet-me Conference VDNs.	All

Creating or changing a Meet-me Conference vector

Procedure

1. Enter `change vector n`, where *n* is the number of the vector that you want to create or change.

   Vector numbers must be between 1 and 256.

2. In the **Meet-me Conf** field, type `y` to designate the vector as a Meet-me Conference vector.

3. Use the numbered fields to create or change a Meet-me Conference vector, as shown in the examples Call Vector screen Page 1 and Call Vector screen Page 2.

   For more information on how to create a vector, see Options for creating vector steps and How the vector processes a call.

```
change vector 90                                              Page  1 of 3

                                 CALL VECTOR

    Number: 90                    Name: Enh Conf Vec
                 Attendant Vectoring? n    Meet-me Conf? y           Lock? y
    Basic? y    EAS? n   G3V4 Enhanced? n   ANI/II-Digits? n   ASAI Routing? n
Prompting? y    LAI? n  G3V4 Adv Routs? n   CINFO? n   BSR? n    Holidays? n

01 collect       6 digits after announcement 12340
02 goto          step 6 if digits = meet-me-access
03 collect       6 digits after announcement 12341
04 goto          step 6 if digits = meet-me-access
05 disconnect    after announcement 12342
06 goto          step 11 if meet-me-idle
07 goto          step 14 if meet-me-full
08 announcement  12343
09 route-to      meetme
10 stop
11 announcement  12344
```

Figure 21: Call Vector screen Page 1

```
 change vector 90                                                Page  2 of 3

                                  CALL VECTOR

    Number: 90                    Name: Enh Conf Vec
                  Attendant Vectoring? n    Meet-me Conf? y           Lock? y
    Basic? y    EAS? n   G3V4 Enhanced? n   ANI/II-Digits? n   ASAI Routing? n
Prompting? y    LAI? n  G3V4 Adv Routs? n   CINFO? n   BSR? n   Holidays? n

12 route-to      meetme
13 stop
14 disconnect    after announcement 12345
15 stop
16
17
18
19
20
21
22
```

Figure 22: Call Vector screen Page 2

4. Press `Enter` to submit the vector.

Note:

If a new party joins a conference immediately, and the party is an H.323 IP trunk user, the caller cannot have a talk path with the other parties in the conference. To prevent this situation, include a short delay in the vector at a point before a new party joins the Meet-me Conference. This delay can be a step to collect digits, a 1-second delay, or an announcement. Since Meet-me vectors are almost always configured with announcements and digit collection, this situation is rarely an issue.

Related links

Options for creating Meet-me vector steps on page 963
Example of how the Meet-me vector processes a call on page 964

Options for creating Meet-me vector steps

collect

When the **Meet-me Conf** field is enabled, the collect vector step collects the next six digits. The vector step then uses those digits as the access code for a Meet-me Conference call. See vector steps 1 and 3 in the example in Call Vector screen Page 1 on page 962.

goto

The goto vector step has three conditions:

meet-me-idle:

The meet-me-idle condition routes the first caller who accesses a Meet-me Conference to the conference call. An announcement step that tells the caller that he is the first party to join the

conference can be played. See vector steps 6 and 11 in the example in Call Vector screen Page 1 on page 962.

meet-me-full:

The meet-me-full condition is used when the Meet-me Conference already has the maximum of six parties on the call. See vector steps 7 and 14 in the example in Call Vector screen Page 2 on page 963.

If the **12–party Conferences** field is enabled in the Feature-Related System Parameters screen, the meet-me-full condition is used when the Meet-me Conference already has the maximum of twelve parties on the call.

meet-me access:

The meet-me access condition ensures that the access code is valid. If the access code that the caller dials is the same as the access code that is administered for the VDN, vector processing continues. See vector steps 2 and 4 in the example in Call Vector screen Page 1 on page 962.

route-to

The route-to vector step has one condition:

meetme:

This condition adds the caller to the Meet-me Conference call, and all parties on the call hear an entry tone. The meetme condition is valid when the caller enters the correct access code, and the number of parties who are on the call already is less than six. See vector steps 9 and 12 in the example in Call Vector screen Page 2 on page 963.

If the route-to meetme step fails, vector processing stops, and the caller hears a busy tone.

Example of how the Meet-me vector processes a call

This section describes what occurs when a caller dials the Meet-me Conference telephone number that is managed by the vector in Call Vector screen Page 1 on page 962 and Call Vector screen Page 2 on page 963.

The caller hears announcement 12340. Announcement 12340 says, “Welcome to the Meet-me Conferencing service. Enter your conference access code.” The caller dials the access code 937821. The collect vector step 1 collects the access code digits. If the access code is valid, the vector processing continues with vector step 6.

If the access code is invalid, vector step 3 plays announcement 12341. Announcement 12341 says, “The access code you entered is invalid. Please enter the access code again.”

If the caller dials the wrong access code again, vector step 5 plays announcement 12342. Announcement 12342 says, “This access code is invalid. Please contact the conference call coordinator to make sure you have the correct conference telephone number and access code. Goodbye.” The caller is disconnected.

Vector step 6 is only valid for the first caller into the Meet-me Conference. The meet-me-idle condition routes the first caller to announcement 12344, according to vector step 11. The announcement says, “You are the first party to join the call.” The system then routes the caller to the Meet-me Conference call by vector step 12, and vector processing stops.

Vector step 7 is used when the Meet-me Conference maximum of six parties are already on the call. The meet-me-full condition disconnects the caller after announcement 12345 plays, according to vector step 14. Announcement 12345 says, “This Meet-me Conference is filled to capacity. Please contact the conference call coordinator for assistance. Goodbye.” If the **12–party Conferences** field is enabled in the Feature-Related System Parameters screen, the meet-me-full condition is used when the Meet-me Conference already has the maximum of twelve parties on the call.

If a caller dials the correct access code, is not the first caller, and the conference is not full, processing continues with vector step 8. Announcement 12343 plays. The announcement says, “Your conference call is already in progress.” The system then routes the caller to the Meet-me Conference call by vector step 9, and vector processing stops.

When a caller enters the conference, all parties on the call hear an entry tone. When a party drops out of the conference, the remaining parties hear an exit tone.

Creating a Meet-me Conference VDN

Procedure

1. Enter `add vdn next`, or `add vdn` *n*, where *n* is the extension that you want to use for the VDN.

   Note that if the VDN extension is one of your Direct Inward Dialing (DID) numbers, external users can access the conference VDN. If the VDN extension is not part of the DID block, only internal callers on the network, or remote access callers, can access the conference.

2. In the **Extension** field, type the extension for the VDN.

   Or, if you typed the extension in Step 1 as part of the **`add vdn`** command, the system automatically displays the extension in the **Extension** field.

3. (Optional) In the **Name** field, type a name of up to 27 characters to identify this VDN.

4. In the **Vector Number** field, type the number for this vector.

   Or, if you typed **`add vdn next`** in Step 1, the system automatically displays the next available vector number in the **Vector Number** field.

5. In the **Meet-me Conferencing** field, type `y`.

6. Click **Next** until you see the Meet-me Conference Parameters page of the Vector Directory Number screen.

7. In the **Conference Access Code** field, assign a 6-digit access code for the Meet-me Conference.

   Avaya recommends that you always assign an access code for a Meet-me Conference. However, if you do not want to assign an access code, leave the **Conference Access Code** field blank. Once you assign an access code, the system displays an asterisk (*) in this field for subsequent change, display, or remove operations by all users except the init superuser login. An administrator who uses the init login sees the actual access code instead of an asterisk.

8. In the **Conference Controller** field, type the extension of the person who is responsible to control or change the Meet-me Conference access code.

   If you type an extension, a user at that extension can use a Feature Access Code (FAC) to change the access code. If you leave the **Conference Controller** field blank, any station user to whom console permissions are assigned can change the access code. Remote access users can also use a FAC to change a Meet-me Conference access code.

9. Select `Enter` to submit the VDN.

End-user procedures for Meet-me Conference

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Accessing a Meet-me Conference as an attendee

Procedure

1. Dial the Meet-me Conference telephone number.

   If an access code is required, a recorded announcement tells you to enter the access code.

2. Enter the Meet-me Conference access code.

   The system verifies the access code, and connects you to the Meet-me Conference. You hear an entry tone when you join the conference.

   If the maximum of six parties are already connected to the Meet-me Conference, a recorded announcement tells you that the Meet-me Conference is full. However, if the **12–party Conferences** field is enabled in the Feature-Related System Parameters screen, and maximum of 12 parties are already connected to the Meet-me Conference, a recorded announcement says that the Meet-me Conference is full.

Changing a Meet-me Conference access code

About this task

Both local and remote access telephone users can change access codes. However, an access code must first be administered through system administration before a telephone user can change a code. Access codes must be removed through system administration.

Procedure

1. Dial the Feature Access Code (FAC) for Meet-me Conference.
2. When you hear dial tone, dial the Meet-me Conference VDN, and then press `#`.
3. Dial the current access code, and then press `#`.

4. When you hear dial tone, dial the new access code, and then press #.
5. Dial the new access code again, and then press #.
6. When you hear the confirmation tone, disconnect the telephone.

Note:

If any errors occur during this operation, you hear intercept tone, and the access code is not changed. You must start over.

Using Selective Conference Party Display, Drop, and Mute

About this task

You can use this feature from a digital display station or from an attendant console. In this example, stations A, C, and D are on a conference call. Caller B is on the conference call that uses an outside trunk or a cellular telephone.

Procedure

1. Station A presses the **Conference Display** button.

   The LED for the **Conference Display** button lights. The station displays the name and the number for station C, if this information is available.
2. Station A can press the **Conference Display** button repeatedly to cycle through all parties who are on the call.
3. When the name and the number for station C is displayed on station A, station A presses the Drop button, or the **Forced Release** button on the attendant console.

   Station C is dropped from the conference call. Callers A, B, and D remain on the conference call. The display for station A now shows one of the other parties on the call.
4. Caller B from an outside trunk puts the conference call on hold.

   This action adds music-on-hold to the conference call.
5. Station A presses the **Conference Display** button until the station displays the name and the number for Caller B.
6. Station A presses the **Far-End Mute** button.

   Note:

   You can activate Far-end Mute only for trunks, and not for telephones.

   Caller B is put into “listen-only” mode, and the music-on-hold is removed from the conference call. The Station A display indicates that the outside trunk call (Caller B) is muted.
7. Caller B selects the conference call appearance to return to the conference call.

   To exit “listen-only” mode, the outside trunk caller presses #.

   Caller B is again active on the conference call.

8. Station A presses the **Exit** button, or the **Normal** button on the attendant console.

   Station A returns to normal mode. Conference 3 is displayed on station A. If station A is inactive for 60 seconds, Station A returns automatically to normal mode.

   If the Selective Conference Party Mute feature is activated without the knowledge of the muted party, that party might think that a problem exists with the connection when no one responds on the conference call. Users must be instructed about this new feature, and how to return to the call if the users are muted. If the muted party does not know how to return to the call, another user on the conference call can use the **Far-End Mute** button to unmute the party.

   Rotary telephone users who are muted by way of the Selective Conference Party Mute feature cannot add themselves back into the conference call. Another user on the conference call must use the **Far-End Mute** button to unmute the party.

Considerations for Meet-me Conference

This section provides information about how the Meet-me Conference feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Meet-me Conference feature under all conditions.

Attendant Intrusion

An attendant can intrude on a station that is part of a Meet-me Conference, as long as the conference does not already include the maximum number of parties.

Bridged Appearances

Bridged appearance users can be added to a Meet-me Conference, and count against the total number of conference parties. As bridged appearance users join a Meet-me Conference, the users are not prompted to provide an access code. Bridged appearance users also receive no announcements, nor are entry or exit tones applied when the users are added to or dropped from the call. Avaya assumes that this scenario would only take place with the knowledge of the user of the appearance that originally dialed into the Meet-me Conference. That user can use the Exclusion feature to prohibit the bridged user from being a part of the Meet-me Conference call.

Busy Verification

If the maximum of stations in a conference call is five or less, a station or an attendant can verify another station that is part of a Meet-me Conference. If the system maximum of stations in a conference call is six, a station or an attendant can verify another station that is part of a Meet-me Conference, as long as the conference does not already include the maximum number of parties.

Call Vectoring

If a Meet-me Conference VDN is administered to use a vector that has no steps, the call attempt is dropped, and a vector event is generated.

Capacity issues

A Meet-me Conference call can have a maximum of six parties on the call. Additional parties cannot join Meet-me Conference once the maximum of six parties is reached. However, if the **12–party Conferences** field is enabled in the Feature-Related System Parameters screen, additional parties can not join Meet-me Conference once the maximum of twelve parties is reached.

Changing vector types

To change a Meet-me Conference vector to a non Meet-me Conference vector, you must first remove all vector steps. To change a non-Meet-me Conference vector to a Meet-me Conference vector, you must first remove all vector steps.

Class of Service (COS)

A user must have a COS that includes console permissions to change a Meet-me Conference access code from his own telephone.

Conference

Parties in a Meet-me Conference call can use the Conference feature to add other parties up to the system conference limit. When the parties are added to the call, the “entry” tone is not given. Two or more Meet-me Conference calls cannot be conferenced together.

Conference Tone

The purpose of the conference tone feature is to ensure that no one can be added to a call without the knowledge of the other parties. The Meet-me Conference already has entry and exit tones for all parties who enter the conference through vector processing. If one of the parties conferences in another user through the station Conference feature, the other parties remain unaware of the additional party because no entry tone is played. In this scenario, the conference tone should be played if required as part of the system parameters administration.

Conference/Transfer Toggle/Swap feature limitations

The Conference/Transfer Toggle/Swap feature is unavailable on analog stations and the attendant console. The attendant console can use the Split Swap feature to perform a similar operation.

The station user who presses the Toggle Swap button must be in the talk state with one of the parties. If the button is pressed during ringback, the system ignores the button push.

Telephone users must not use the Selective Conference Party Display feature to scroll too rapidly through the displays. The station hyperactivity feature takes the station out of service if the user repeatedly scrolls through the displays at high enough rates. This action causes the system to reset, and drop the user from the call.

Disabling Enhanced Conferencing

To disable the Enhanced Conferencing option on the System Parameters Customer- Options screen, you must first remove all Meet-me Conference VDNs and vectors.

Drop

No controlling party exists in a Meet-me Conference. Therefore, if a caller who is on the conference call presses the Drop button, the system ignores the button push, and the last party who joined the conference call is not dropped from the call.

Far-end Mute

Only one trunk on a Meet-me Conference bridge can be far-end muted at any given time.

Removing stations

You cannot remove a station that is administered as a controlling station for a Meet-me Conference VDN unless you first remove the assignment on the VDN.

Security issues

The Meet-me Conference feature can present a potential security problem. If you assign Meet-me Conference VDNs without access codes, a hacker can gain control of Meet-me Conference facilities and keep others from conducting legitimate business. A hacker can also potentially access the system, and use the system to make unauthorized calls. Avaya recommends that you administer access codes, and change the codes regularly to reduce the risk of unauthorized access to the system. If a user tries to change the access code of a Meet-me Conference and is unsuccessful, or uses an invalid access code, the system records an event to the Event Log.

Service Observing

Service Observing by way of the VDN is not supported for Meet-me Conference VDNs.

Transfer

When a user transfers a call to a Meet-me Conference, the transfer can be completed during vector processing only when a single party is on soft hold and waiting to be transferred. If two or more parties are on soft hold and waiting to be transferred, the transfer can only be completed after the party who initiates the transfer is connected to the Meet-me Conference.

Vectoring options

Attendant Vectoring and Meet-me Conference cannot both be enabled at the same time. If Enhanced Conferencing is enabled, but no other vectoring customer options are enabled, only Meet-me Conference vectors can be assigned. A non Meet-me Conference vector cannot be assigned to a Meet-me Conference VDN. A Meet-me Conference vector cannot be assigned to a non-Meet-me Conference VDN. No restrictions exist with regard to vector “chaining” between Meet-me Conference vectors and non Meet-me Conference vectors. When a call interflows from one type of vector processing to another, the call is removed from any queue, if applicable. The call is treated as a new call to vectoring, instead of a continuation of vectoring.

Interactions for Meet-me Conference

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

Call Detail Recording (CDR)

As parties join a Meet-me Conference, a call record is created, if a record is required by system administration. If a record is required, the called party is the Meet-me Conference VDN number. The duration is the length of time that the party is included in the call. An individual record for each party is generated when the party drops from the call.

One option for recording all calls to Meet-me Conference VDNs is to activate the Intraswitch CDR feature, and populate all system Meet-me Conference VDN numbers. If you use the Intraswitch CDR feature with the Meet-me Conference VDNs, set the condition code to C for all call records.

If the Intraswitch CDR feature is inactive for Meet-me Conference VDNs, the creation and the content of call records depends on the trunk group translations for external callers to the Meet-me Conference. Internal callers to the Meet-me Conference do not generate any records if the Intraswitch CDR feature is inactive for either the Meet-me Conference VDN or the calling extension.

Direct Inward Dialing (DID)

If a Meet-me Conference VDN is one of your block of DID numbers, external users can access the conference VDN. If the VDN extension is not part of the DID block, only internal callers on the network or remote access callers can access the conference VDN.

Troubleshooting Meet-me Conference

This section lists the known or common problems that users might experience with the Meet-me Conference feature.

Problem	Possible cause	Action
The conference call drops abruptly for no apparent reason.	The **Vector Disconnect Timer** field on the System Parameters - Features screen is set to a value that is shorter than the duration of the Meet-me Conference session.	Increase the value in the **Vector Disconnect Timer** field.
The sound volume is too low.	The affected conference participants connect through international trunks in which central office (CO) loss plans are set for too much loss.	• Speak closer to the speaker phone. • If you are having conference calls in a large conference room, then use a microphone for the speaker. You can also use Polycom phones that have automatic gain control. • On the Location Parameters screen, adjust the values in the **End-to-End total loss (db) in a n-party conference** field. The loss can be as low as 15DB.

Chapter 124: Multifrequency Signaling

Use the Multifrequency (MF) signaling feature to perform signaling used between media servers and the Central Office (CO). It is similar to dual-tone multifrequency (DTMF) signaling in that tones convey the dialed number.

With MF signaling, the signal is usually a combination of two frequencies from a group of 5 or 6 frequencies (2/5 or 2/6). The origination and destination servers or switches exchange tones that have specific meanings according to the MF protocol.

Detailed description of Multifrequency Signaling

Communication Manager supports two frequency groups:

- R2-multifrequency compelled signaling (R2-MFC) frequency
- R1 frequency (for Spain and Russia)

R2-MFC is a version of MFC recommended by the International Telecommunication Union (ITU). It provides signaling between a CO and a media server over analog or digital CO, Direct Inward Dialing (DID), or Direct Inward and Outward Dialing (DIOD) trunks. It also provides signaling between any 2 servers running Communication Manager.

Communication Manager provides MF signaling that complies with ITU regulations and national regulations for specific countries. It provides these types of MF signaling: MFE MF Shuttle, and multifrequency compelled (R2-MFC). These protocols signal the called number, the calling party's number (ANI), and information about the type of call or type of caller (category).

Communication Manager supports prefix digits for ANI sent on outgoing calls to be defined per server, or per the originator's class of restriction.

If a call is a tandem call and the incoming and outgoing trunk use different protocols, Communication Manager makes no attempt to convert between the various protocol's meanings for category. Instead,

- the server uses the incoming trunk's COR assigned category if the outgoing trunk is Russian or R2-MFC, and
- the server uses ARS call types if the outgoing trunk is MFE.

The server running Communication Manager provides the incoming ANI to all features on Communication Manager that need to identify the calling party.

MFE

MFE, for Country code 11 (Spain), uses R1 frequency and compelled signaling. It is available on CO and DID trunk groups. There are four types of MFE signaling:

- Public 2/5
- Public 2/6
- Ibercom 2/5
- Ibercom 2/6

MF Shuttle

MF shuttle signaling, for country code 15 (Russia), uses R1 frequency and noncompelled signaling. With MF shuttle signaling, it is possible to change to decadic rotary pulse in the middle of address signal exchange. MF shuttle signaling is available on CO, DID, and DIOD trunk groups.

Also, ANI transmission, for Country code 15, uses a gapless R1 MF signal and is completed within 800ms. This is available on an outgoing CO trunk group.

R2-MFC

Each country can use R2 multifrequency compelled (R2-MFC) signaling to define the meanings of the R2 frequency combinations.

Guidelines for administering Multifrequency Signaling

To administer MF signaling, you must first identify the origination and destination server or media servers. The one making the call is the origination server. The one answering the call is the destination server.

- The origination server or media server creates forward signals, classified as group I and group II signals.
- The destination server or media server creates backward signals, classified as group A and group B signals.

Group I and group A signals comprise the basic signaling for the dialed number. More elaborate signaling requires Group II and group B signals. Signal meanings and timer values can be administered.

The following sequence shows a typical interaction between the origination server (forward group I and group II signals) and destination server (backward group A and group B signals).

Forward			Backward
Group I	digit	-->	
	<--	A.1	Group A
	digit	-->	

Table continues…

Forward			Backward
	<--	A.1	
	digit	-->	
	<--	A.1	
	digit	-->	
	<--	A.1	
	digit	-->	
	<--	A.3	End of dial
Group II	II.2	-->	
	<--	B.x	Group B

Second, you assign the correlation between signal codes and their meanings.

1. Assign a code to each message. The code consists of a group category, like group II or A, and a number.
   - For example, you might assign code A.1 to the message “next-digit”.
2. Assign a signal to each identifying code.
   - In every country, the frequencies (levels might differ by country) assigned to the identifying codes are the same. However, the messages assigned to the identifying codes can be different.

     For example, in Switzerland the B.6 code and its associated signal convey the free message, while in Thailand, free is conveyed by the B.1 code and its associated signal. But in both Switzerland and Thailand, the frequency associated with the B.1 code is the same.

     As another example, you might assign the signal “busy” to the B.1 code.

To receive Russian incoming ANI:

- On the DID or DIOD Trunk Group screen, set the **Country** field to 15 and the **Protocol Type** field to inloc.
- On the AAR and ARS Digit Analysis Table screen, set the **ANI Req** field to y, or on the AAR and ARS Digit Conversion Table screen, set the **ANI Req** field to y.

Multifrequency Signaling administration

This section describes the screens for the Multifrequency Signaling feature.

Screens for administering Multifrequency Signaling

Screen name	Purpose	Fields
Multifrequency-Signaling Related Parameters	Sets the system parameters for multifrequency signaling	All
AAR and ARS Digit Conversion Table	Sets automatic number identification	ANI Reqd
AAR and ARS Digit Analysis Table	Sets automatic number identification	ANI Reqd

Considerations for Multifrequency Signaling

This section provides information about how the Multifrequency Signaling feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Multifrequency Signaling under all conditions. The following considerations apply to Multifrequency Signaling.

The following considerations apply to R2-MFC only:

- Both non-group II signaling and group II signaling are supported on incoming MF signaling calls. The group II signaling protocol has an extra signal that provides caller-category information. Only group II signaling is supported on outgoing MF signaling calls.
- MF signaling also can be used in tandem trunk groups. After address signals are collected from an incoming group II MF signaling call, the call can route to a group II MF signaling trunk.
- Both incoming and outgoing MF signaling calls support ANI displays, ANI information and the CDR records the information.
- When Communication Manager uses an open numbering plan, the end-of-dial signal must be defined in the incoming Group I signal administration. After sending all address digits, the CO sends the end-of-dial signal to Communication Manager.
- If Communication Manager makes an outgoing call to the CO that uses an open numbering plan, the CO must send the signal A.1 to Communication Manager after sending the last address digit to the CO. Then, the CO should time out and send a pulsed signal A.3 to Communication Manager requesting the Group II signal.
- Communication Manager offers the option to record the Calling Party Category in the CDR. For incoming external calls, this comes from the Group II signal. For internal calls and station-originated external calls, this comes from the COR of the originating station. For tandem calls, this value comes from the Group II signal, determined by the COR of the originating trunk group. The CDR device is capable of receiving this information.
- You can assign Calling Party Category and Called Party Category on a trunk-by-trunk basis.
- You can record an announcement to play when outgoing R2-MFC trunk calls do not complete. This applies when Communication Manager receives either group A or B signals from the called Central Office or other media server or switch.

Interactions for Multifrequency Signaling

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

ASAI

ANI collected from incoming R2-MFC signaling can be used with ASAI.

Abbreviated Dialing

Although calls dialed automatically from an abbreviated dialing privileged list complete without COR checking, ANI prefix and ANI truncation still apply.

Attendant Console

If the attendant assists or extends a call for a station using Straightforward Outward Completion and Through Dialing, and if the attendant has not yet released the call when the request for ANI comes in from the far end, the attendant's COR is used to select the ANI for the call. If the attendant has already released the call when the request for ANI comes in from the far end, the attendant's COR is used to select the ANI for the call.

Authorization Codes

The COR of the authorization code as administered on the authorization-code screen is not used for ANI prefix determination, even if the originating endpoint enters an authorization code before call processing for an outgoing call seizes an outgoing trunk. If the originating endpoint is an extension, the extension's ANI is used. If the originating endpoint is an incoming trunk, the ANI for PBX is used.

Bridging

The ANI of a telephone's primary extension also applies to calls originated from a bridged call appearance of that extension on another terminal. ANI prefix and ANI truncation applies to the primary extension number of bridged call appearances.

Call Detail Recording (CDR)

CDR records ANI collected from incoming MF signaling.

For India MFC, on incoming calls, ANI digits may be appended with zeroes if the actual ANI digits are less than the administered ANI-length. In these calls, CDR displays the zero digits.

Call Redirection

A call is redirected if any of the following are active: Call Forwarding, Call Coverage, Send All Calls, or Night Service.

Call Vectoring

Call Vectoring can now use ANI collected from incoming MFC signaling.

The ANI of a call vector is not used when a call vectoring route-to command routes a call over an outgoing trunk. Instead, the ANI of the originating party is sent.

DID No Answer Timer

DID No Answer Timer is applied to MF signaling DID calls.

Distributed Communications System (DCS)

In a DCS arrangement, the ANI sent to the CO is determined by the ANI for PBX on PBX_B, but the category sent to the CO is determined by the Category for MF ANI field on the Class of Restriction screen for the incoming DCS trunk or by the type of call.

Expert Agent Select (EAS)

For ANI, the EAS agent's login extension number and COR overrides the extension number and COR of the physical terminal where the agent is logged in. ANI prefix and ANI truncation apply to logged in EAS agents.

Hunt Groups and Automatic Call Distribution (ACD) Splits

For ANI, a physical terminal's extension number and COR overrides the extension number and COR of the hunt group or ACD split that is a member of or logged into. ANI prefix and ANI truncation apply to terminals that are members of hunt groups or logged into ACD splits.

Intercept treatment

For DID MF signaling calls that are denied, you can administer whether the corresponding B.x signal or intercept tone should be sent to the CO. The default is to send the administered DID/TIE/ISDN Intercept Treatment. If the option to send the B.x signal is set, then:

- For Group II calls, the B.x signal for the intercept is sent to the CO.
- For non-Group II calls, if the CO dials an invalid number, the trunk is locked (regardless of this option). If the CO dials a number that is valid but unassigned, intercept tone is sent to the CO.

Multimedia Call Handling (MMCH)

For call origination, multimedia complexes use the COR assigned to their telephones. ANI prefix and ANI truncation will apply to the telephones assigned to multimedia complexes.

Off-Net Call Coverage or Call Forwarding

If the originating endpoint is an extension, the extension's ANI is used. If the originating endpoint is an incoming trunk that can supply ANI, the ANI received from the incoming trunk is used. If the originating endpoint is neither of the above, the ANI for PBX is used.

Personal Station Access (PSA)

For ANI, the PSA extension number and COR overrides the extension number and COR of the physical terminal where the PSA extension number is associated. ANI prefix and ANI truncation will apply to associated PSA extension numbers.

Remote Access

The COR of a remote access barrier code is not used for ANI prefix determination when the originating end point dials a remote access extension and then places a call. If the originating endpoint is an extension, the extension's ANI is used. If the originating endpoint is an incoming trunk, the ANI for PBX is used.

Station Set Displays

When no ANI is possible, if station sets are equipped with display option, they do not display the ANI digits. Instead, the trunk group name displays. When ANI is possible, ANI displays on the station set.

Note:

For India Only. If ANI digits are padded with zero, then zeroes also are displayed along with ANI digits.

Tandem/Offnet Calls

If ANI digits are received on incoming MFC calls, the ANI digits are sent to outgoing tandem/ off-net calls.

Note:

For Russia Only. The ANI is requested on incoming trunks only when all the address digits have been collected. When the incoming trunk on a tandem call is a Russian incoming local trunk administered to collect ANI, the server collects all ANI digits before seizing the outgoing tandem trunk. This happens even if ARS is administered with a min value low enough that it would be possible to determine an outgoing route through digit analysis.

Note:

For India Only. On an outgoing tandem-call, the default operation is to send the ANI-Not-Available forward signal if ANI is unavailable from the incoming trunk. However, to support this operation, leave the **ANI for PBX** field blank, and define the ANI-Not-Available signal.

Chapter 125: Multi-Device Access

With the Multi-Device Access (MDA) feature, a SIP user can register more than one SIP device with a single extension. For example, a user has 96X1 at his desk, 96X1 in his lab, and Avaya one-X® Communicator on his laptop and all the devices are registered with the same extension 123456. When a call arrives at extension 123456, all the devices are alerted. The user can answer the call from any one of the devices. If required, the user can bridge on to the call from one of the idle devices by using the Simulated Bridge Appearance (SBA) feature. Therefore, the call can be handed off between devices without parking the call. A user can register up to 10 SIP devices with the same extension.

Related links

Detailed description of Multi-Device Access on page 979
Interactions for Multi-Device Access on page 980

Detailed description of Multi-Device Access

The devices registered in the Multi-Device Access (MDA) group, inherit the properties of the extension configured on Communication Manager. However, the support of the feature buttons differ from one device to another.

When one of the MDA devices answers the incoming call, Session Manager cancels the call request to other MDA devices. The inactive devices can join the call by using the Simulated Bridged Appearance (SBA) feature. However, Communication Manager does not change the call display to *conference*. The MDA devices display the call as a two-party call. This feature of joining a call is known as Multi-Device Access.

When all the MDA devices receive a call, only one device can answer the call. However, multiple MDA devices can send a provisional response about sending early media, for example, a ringback or an announcement.

The Hold and Active states are managed for all the registered devices irrespective of whether the devices are active or idle. For example, when one of the MDA devices places the call on hold, the call remains in the active state till other MDA devices active on the call also change the call state to *hold*.

If an MDA device is active on a call and tries to join the call by using one of the other MDA devices, Communication Manager checks the status of the Exclusion feature setting. If the feature

is active, the devices cannot join the call until the exclusion feature is deactivated by the MDA device user who activated it.

Related links

Multi-Device Access on page 979

Interactions for Multi-Device Access

Attended and unattended Transfer

If multiple devices are connected to a call, and one of the devices transfers the call, Communication Manager disconnects all the devices from the call when the transfer is complete. If a user with multiple devices transfers a call and the call returns back to the station through the Transfer Recall feature, Communication Manager alerts all the MDA devices.

Hold Unhold

Users can put an active call on hold from an MDA device while another MDA device is still active on the call. Communication Manager activates hold-based features, such as Hold Recall, if all the devices are on hold.

Conference

When MDA devices bridge on to a call and one of the devices completes a conference, other MDA devices might get dropped from the call. The dropped MDA devices can join the conference call again by using the simulated bridged appearance.

Message Waiting Indication Lamp

MDA devices support Message Waiting Indication (MWI) lamps for self and other stations or groups to which the MDA device has subscribed.

Bridging and Exclusion

MDA devices can directly bridge on to a non-ACD call by selecting a call appearance on which a call is already active or by having two devices bridge on to the same bridged appearance of an independent extension.

MDA devices cannot directly bridge onto an ACD call.

MDA for SIPCC has the following restrictions:

- The SIP agent must be registered and logged into only one physical endpoint.
- Soft clients using Third Party Call Control (3PCC) must operate in shared control mode. For example, if Avaya Equinox is used, Equinox must be configured to operate in “My Desk Phone” mode.

Registering two endpoints to the same extension is permissive use and will cause functional interactions during feature operation. The following examples are the most likely interactions:

- Service Observing will not start when more than one physical endpoint is registered with the same extension.
- Supervisor Assist fails when more than one physical endpoint is registered with the same extension.

Busy Line Indicator and Team Button

If another user has Team button configured for the MDA extension, pressing the Team button alerts all MDA devices.

Call pickup

Call pickup can be initiated from any of the MDA devices. A call alerting at an MDA device that is picked up by another user causes the MDA devices to stop alerting.

Call park

Call park can be initiated from any of the MDA devices. If an MDA device is on a call with multiple devices and initiates call park at one device, the other devices remain on the call until the MDA devices decide to disconnect the call. An MDA device user can unpark a call from the same device or a different device by using the call unpark feature.

Send All Calls and Call Forwarding

Any MDA device can activate the redirection feature, such as SAC or Call Forwarding. The respective button lamps are lit on all the MDA devices.

Call Log

If a call is answered by an MDA device, the system displays the call in the Answered Call log of that MDA device and in the Missed Call log of the other MDA devices.

Contacts

The contacts of an MDA device are synchronized across other MDA devices. Any change of contact details in an MDA device are reflected across other MDA devices.

EC500

If a user is configured as an MDA group and has one or more EC500 configurations, the configuration is shared by all MDA devices.

Group Page

Depending on the highest Q-value, Session Manager tandems the Callers INVITE message to only one of MDA devices. If more than one device accepts the message at the same time, Session Manager sends the INVITE message to the MDA device that is registered most recently.

Automatic Callback

If a user with multiple devices activates automatic call back, all the registered devices are alerted when the monitored station becomes available. Answering the callback call initiates a new call to the original called party.

Whisper Page and Service Observing

An MDA device can initiate a whisper paging call or activate the Service Observing feature.

ASAI

MDA is not supported for users with multiple devices in Contact Center environments.

Emergency Calls

If an MDA device places an emergency call, Session Manager routes the call directly to the emergency services, depending on the location of MDA. If IP address in the bottom-most

Via header does not match an administered location pattern, Session Manager reverts to the administered home location of the user, as administered in the user communication profile.

Hotel feature

In a hotel room arrangement, multiple devices can connect to a call simultaneously. When placing an outgoing call, only one device must be active until at least all digits have been dialed.

Related links

Multi-Device Access on page 979

Chapter 126: Multi-Location Dial Plan

Use the Multi-Location Dial Plan feature to preserve dial plan uniqueness for extensions and attendants when you migrate to a single duplex system distributed network. Without this feature, dial plan uniqueness is not preserved when you migrate from multiple QSIG or distributed communication system (DCS) networks.

Migrating to a single distributed network reduces the number of systems you must maintain. With a single network, you administer one system and one dial plan. However, with a single distributed network, some features no longer work transparently across multiple locations as before the migration.

For example, in multiple QSIG or DCS networks, each location of a department store might have its own system. Therefore, the same telephone extension might represent a unique department in all stores. Extension 4321 might be the luggage department in all stores. Store employees at any location can dial 4321 and get the luggage department in the store.

If you migrate to a single distributed network, store employees can no longer dial 4321 to reach the local luggage department. The system cannot correctly analyze the digits and route the call to the correct store. Store employees now have to dial a complete telephone extension to reach the luggage department in the store.

This problem is solved with the Multi-Location Dial Plan feature. With the Multi-Location Dial Plan feature, Communication Manager adds the location prefix digits to the front of the dialed number. The software then analyzes the entire dialed string and routes the call based on the administration on the Dial Plan Parameters screen.

With the Multi-Location Dial Plan feature, a user can dial a shortened version of an extension instead of having to dial a complete extension. For example, the store employee can continue to dial 4321 instead of having to dial 765-4321 to reach the luggage department.

Note:

Beginning with Communication Manager Release 5.0, you can use different length short number extensions for different locations.

Without the Multi-Location Dial Plan feature in a single distributed network, a call that is routed to an attendant might not terminate at the local attendant. For example, if a school district migrates to a single distributed network, dialing the attendant access code may not route the call to the local school attendant. With the Multi-Location Dial Plan feature, the system can route an attendant-seeking call to a local centralized answering point (LCAP), such as a local station or an attendant console. However, the normal attendant features like system attendant queues are unavailable in such instances.

The Multi-Location Dial Plan feature provides dial plan capabilities that are similar to those of QSIG networks or DCS networks. These capabilities include:

- Extension uniqueness
- Announcements for each location
- Local attendant access
- Local Automatic Route Selection (ARS) code administration

On Linux platforms only, the Multi-Location Dial Plan feature also enhances the dial plan and the Uniform Dial Plan Table screen so that users can:

- Dial a shortened version of a telephone extension, and reach the same destination as before the migration
- Dial and reach a centralized local answering point
- Dial a local attendant Feature Access Code (FAC) or ARS FAC, and access the same feature as before the migration

On Linux platforms only, you can also play administered announcements in a language that is based on location.

Detailed description of Multi-Location Dial Plan

With the Multi-Location Dial Plan feature, users in a single distributed network can dial a local extension to reach a number in their area. Before this can happen, the administer must first retranslate their dial plan and extensions. This feature inserts leading digits from the calling number to the called number for intralocation dialing.

This feature also provides a local centralized answering point for attendants. Finally, with this feature, you can administer multiple Feature Access Codes for ARS and for attendants.

Multi-Location Dial Plan prefix

A new value is available in the **Insert Digits** field on the Uniform Dial Plan Table screen. This new value takes the location prefix of the caller from the Locations screen. The software adds the location prefix to the front of the called number. The software then analyzes the entire dialed string, and routes the call based on the administration on the Dial Plan Parameters screen.

- Non-IP telephones and trunks inherit the location number of the cabinet, the remote office, or the gateway to which they are connected.
- IP telephones and trunks obtain their location number indirectly.
  - On the Network Region screen, you administer a location number that applies to all telephones in that IP region. If a location field is left blank on the Network Region screen, an IP telephone obtains its location from the location of the cabinet that contains the C-LAN board.

- IP trunks obtain the location from the location of their associated signaling group.

  Either direct administration, which is only possible for remote office signaling groups, or the ways described for IP telephones, determines the location.

If the location prefix is not administered correctly, the software does not route calls correctly. A location prefix is not administered correctly if:

- You administer the prefix with incorrect digits
- The entry on the Uniform Dial Plan Table screen does not match the length of the location prefix

Multi-Location Dial Plan Feature Access Codes

- The software uses the **Auto Route Selection (ARS) - Access Code** fields on the Feature Access Code (FAC) screen when no value exists in the **ARS FAC** field on the Locations screen. If a value exists in the **ARS FAC** field on the Locations screen, the software uses that location ARS FAC. The **Auto Route Selection (ARS) - Access Code** fields on the Feature Access Code (FAC) screen are ignored.

  If you use the **ARS FAC** field on the Locations screen, you lose the ability to administer two ARS codes on the Feature Access Code (FAC) screen.

  The location ARS FAC is accessible only for calling numbers at locations that are administered with that ARS FAC. The software denies any attempt to use an ARS FAC at a location for which the FAC is invalid.

- The **Attendant Access Code** field on the Feature Access Code (FAC) screen has the same characteristics as the attd call type on the Dial Plan Analysis Table screen.

  You can administer only one attendant code. You can administer the attendant code either on the Dial Plan Analysis Table screen, or on the Feature Access Code (FAC) screen. You cannot administer the attendant code on both screens.

  If you want to:

  - Administer an attendant access code for different locations, use the **Attendant Access Code** field on the Feature Access Code (FAC) screen.
  - Use one attendant code for all locations, administer the code as attd in the **Call Type** field on the Dial Plan Analysis Table screen.

    You cannot reuse the value that you use for the attd call type for any FACs. Nor can you reuse the value for the ARS FAC or Attd FAC on the Locations screen.

  Attd FAC, the attendant code on the Locations screen, is accessible only for calling numbers at locations that are administered with that attendant access code. The software denies any attempt to use an attendant code at a location for which the code is not valid.

- Only one attendant or ARS access code is valid for a location. The global ARS access code and the attendant access code, and the dialed string for the attendant call type, are valid for a location only if:
  - A local ARS access code does not exist, or
  - An attendant access code does not exist

Multi-Location Dial Plan announcements

With multiple QSIG or DCS networks, multiple switches can handle announcements in multiple languages. Without the Multi-Location Dial Plan feature in a single distributed network, the software cannot play announcements in multiple languages.

With the Multi-Location Dial Plan feature, announcement extensions are stored as digit strings. The software routes these digit strings through Uniform Dial Plan (UDP) processing. This processing is similar to dialing a telephone extension. When the software dials a shortened extension for an announcement, the software prepends the location prefix onto the extension. With both the location prefix and the extension, the software can play the announcement to the caller in the proper language.

Multi-Location Dial Plan invalid announcements

The software provides intercept treatment if the following announcements are invalid:

- DID/Tie/Intercept
- Controlled Outward Restriction Intercept Treatment
- Controlled Termination Restriction (Do Not Disturb)
- Controlled Station to Station Restriction
- Controlled Toll Restriction Intercept Treatment
- Invalid Number Dialed Intercept Treatment

The software skips and does not play the following announcements if the announcements are invalid:

- Analog Busy Auto Callback
- Direct Agent Announcement Extension
- Hospitality

The treatment for an announcement that is invalid during vector processing is the same as if the announcement did not exist. Call processing continues and does not wait. Any previous feedback that precedes the announcement continues.

- An announcement step continues at the next step.
- A wait step that references an announcement continues after any specified wait treatment expires.
- A disconnect step disconnects immediately.

- A collect step continues at the next step.

If the VDN of Origin Announcement (VOA) does not exist, vector processing bypasses the VOA, and delivers the call to the agent.

Multi-Location Dial Plan maintenance

When you migrate to a single distributed network, you must re-administer your dial plan if you want to maintain extension uniqueness. You can administer the UDP so that users can dial a local extension at an individual location the same as before the migration.

If you administer local ARS FACs on the Locations screen, you lose the ability to administer two ARS codes. The ability to administer two ARS codes is currently provided only on the Feature Access Code (FAC) screen.

Multi-Location Dial Plan administration

The following tasks are part of the administration process for the Multi-Location Dial Plan feature:

- Changing extensions when implementing a Multi-location Dial Plan
- Prepending numbers to the dialed string with Multi-Location Dial Plan
- Announcements administration with Multi-Location Dial Plan
- Local centralized answering point administration with Multi-Location Dial Plan
- Multiple Feature Access Code administration for Multi-location Dial Plan attendants
- Multiple Feature Access Codes administration for ARS with Multi-Location Dial Plan

Related links

Multiple Feature Access Codes administration for ARS with Multi-Location Dial Plan on page 992
Multiple Feature Access Code administration for Multi-location Dial Plan attendants on page 991
Local centralized answering point administration with Multi-Location Dial Plan on page 991
Announcements administration with Multi-Location Dial Plan on page 990
Prepending numbers to the dialed string with Multi-Location Dial Plan on page 990
Changing extensions when implementing a Multi-location Dial Plan on page 988

Preparing to administer Multi-Location Dial Plan

Procedure

1. On the Optional Features screen, ensure that the **Multiple Locations** field is set to y.

   If you set this field to n, your system does not support the Multi-Location Dial Plan feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Multi-Location Dial Plan, or to open a service request.

To view the Optional Features screen, enter `display system-parameters customer-options`.

2. On the Daylight Savings Rules screen, ensure that rules for daylight savings time are administered.

   To view the Daylight Savings Rules screen, enter `change daylight-savings-rules`.

   For a complete description of the many Optional Features screens, and the Daylight Savings Rules screen, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Multi-Location Dial Plan

Screen name	Purpose	Fields
Optional Features	Ensure that the multiple locations feature is enabled.	Multiple Locations
Daylight Savings Rules	Ensure that rules for daylight savings time are administered.	All
Locations	• Set up a FAC to access ARS for a location. • Set up a FAC to access an attendant for a location. • Include the prefix for the specific location.	• ARS FAC • Attd FAC • Prefix
Change Station Extension	Change multiple extensions in the software from one extension to another simultaneously.	All
Uniform Dial Plan Table	Set up your dial plan.	All

Changing extensions when implementing a Multi-location Dial Plan

About this task

You can change multiple extensions in the software from one extension to another, simultaneously.

Procedure

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

   Caution:

   The Change Station Extension screen does not change the emergency location extension that is administered within the system. You cannot use this screen to change an extension that is administered as an emergency location extension on either the Station screen or the IP Address Mapping screen.

2. In the **TO EXTENSION** fields:
   a. Type a new extension that you want the current extension changed to.
   b. Type a new extension for the message lamp extension.
   c. Type a new extension for the emergency location ext. field
   d. In the **IP Parameter Emergency Location** field, the system displays the words See IP-Network Map Form.

      You can change the **IP Parameter Emergency Location** field only on the IP Address Mapping screen. Use the **`change ip-network-map`** command.
3. Press `Enter` to save your changes.

Change extension results with Multi-location Dial Plan

When you complete and submit the Change Station Extension screen, all administration that was associated with the previous extension is now associated with the new extensions. This administration includes any references used in a vector, in coverage, and elsewhere in the system. Once you change an extension, the software removes all references to the previous extension.

If you change an extension that is also administered on an adjunct, you must also change the extension on the adjunct. Examples of adjuncts include voice mail and an Adjunct-Switch Application Interface (ASAI) link.

Exceptions

- The **`change extension-station`** *n* command does not change the administration that is associated with call forwarding digits and abbreviated dialing buttons on the current extension.
- To change a forwarded extension that is administered as a button, do not use the **`change extension-station`** *n* command. The extension for the call forwarded button is stored as digits rather than as a UID. Avaya recommends that you use the **`list usage`** command before you change any extensions.
- The **`change extension-station`** *n* command does not update the **ISDN BRI SPID** field for BRI telephones. To update this field, you must make manual changes on both the switch and the telephone.

Audits

- If you try to change an extension that is administered on the same switch as an emergency location extension on the Station screen or on the IP Address Mapping screen, the system displays the following warning message:

  Extension exists as Emergency Location. Continue?

  Click **yes** to process the change. Click **no** to stop the process.
- The **`change extension-station`** *n* command is be denied under the following conditions:
  - If the extension being changed is active on a call
  - If the administrator is accessing the extension

- If you attempt to change an extension that is administered on the same system as a media complex extension on the Station screen, the extension cannot be changed to a 6-digit or 7-digit number. The **media complex extension** field on the Station screen does not support 6-digit or 7-digit numbers.

  For example, extension 50002 is an IP (H.323) telephone extension. Extension 50002 is administered on extension 51234 as the media complex. You cannot use the **`change extension-station`** *n* command to change extension 50002 to 7050002 because the software does not support a 7-digit media complex number. You can, however, use the command to change 50002 to 52222, because 52222 is a 5-digit extension.

Prepending numbers to the dialed string with Multi-Location Dial Plan

You can use this software to enter a new value in the **Insert Digits** field in the Uniform Dial Plan Table screen. The value is Lx. In the value Lx, *x* indicates a number from 1 to 5. The number *x* must match the number of digits in the **Prefix** field on the Locations screen. For example, if the **Prefix** field on the Locations screen contains three digits, assign the value L3.

When you use the value Lx in the Uniform Dial Plan Table screen, the software takes the value in the **Prefix** field from the Locations screen, and prepends the number of digits to the dialed string.

To prepend numbers to the dialed string:

1. Enter `uniform-dialplan` *n*, where *n* is the number of the dial plan.
2. In the **Insert Digits** field, type `L` and a number from 1 to 5. The number that you type must equal the number of digits in the **Prefix** field on the Locations screen. This number is the number of digits that the software prepends to the dialed telephone number.

   For more information on the Uniform Dial Plan Table screen, see *Administering Avaya Aura® Communication Manager*.
3. Press `Enter` to save your changes.

Announcements administration with Multi-Location Dial Plan

In addition to the shortened extensions, you must also administer announcements. If your organization has multiple locations with announcements in multiple languages, you must administer the announcement for each location, even if many of the announcements are identical.

For example, if your organization has 100 locations, announcements in 90 locations are in English. In the remaining 10 locations, announcements are in non-English languages. You must administer announcements in all 100 locations, even if 90 of the locations use the same English announcements.

For some announcements, such as the DID/Tie/Intercept announcement, you can administer only a single announcement. This restriction can create a problem in a single distributed network. For example, a duplex Media Server might support multiple countries, and therefore require that announcements play in the language of the country. This example poses a problem because you can only administer a single announcement.

To accommodate several announcements that share a single administered field, use the Multi-Location Dial Plan feature. With the Multi-Location Dial Plan feature, the announcement that plays is based upon the calling number, and the **Location Prefix** field on the Locations screen.

For example, 4567 is the extension administered in the **DID/Tie/ISDN Intercept Announcement** field on the System Features screen. You can record multiple announcements for extension xxx-4567:

- 420-4567 in English
- 813-4567 in German
- 964-4567 in French
- 371-4567 in Spanish
- 628-4567 in a user-defined language

You must administer all announcements - 420-4567 in English, 813-4567 in German, 964-4567 in French, 371-4567 in Spanish, and 628-4567 in the user-defined language. When a person calls and is about to hear announcement 4567, the system inserts the prefix digits based on the location of the caller. The system then plays announcement 4567 in the proper language.

Local centralized answering point administration with Multi-Location Dial Plan

With the Multi-Location Dial Plan feature, you can use vector routing or hunt groups to set up a local centralized answering point (LCAP). The LCAP gives users access to a local attendant.

With vector routing, you can administer a VDN with extension “0” with a vector “route-to” step for a shorter extension. You then administer the Uniform Dialing Plan screen with an entry for the shorter extension in the vector step. The purpose is to prepend digits from the calling party number. The system routes the call to the extension that you designate as the LCAP.

You can also use a hunt group to set up an LCAP. You administer the Uniform Dialing Plan screen so that the shorter extension for the hunt group prepends digits for the calling party number. One of the members of a local hunt group can be designated as the LCAP.

Note that if you use an LCAP, you cannot also use local access codes. LCAPs and multiple Feature Access Codes for the attendant are mutually exclusive.

Multiple Feature Access Code administration for Multi-location Dial Plan attendants

Without the Multi-Location Dial Plan feature, you can administer only one attendant Feature Access Code (FAC) on the Dial Plan Analysis Table screen. With this feature, you can administer multiple attendant FACs. The Multi-Location Dial Plan feature adds the administration of the attendant dial access code to the Feature Access Code (FAC) screen. The call type is attd. With this change, different locations can share the value that is used for the attendant access.

For example, you might enter the access code 9 for ARS on the Feature Access Code (FAC) screen. You might then enter the attendant access code on a Locations screen as 8. When a user dials 8 from that location, the software routes the call to an attendant.

Only one attendant group can exist in the software at a time.

Multiple Feature Access Codes administration for ARS with Multi-Location Dial Plan

Without the Multi-Location Dial Plan feature, you can administer only two attendant FACs on the Feature Access Code (FAC) screen. With this feature, you can administer multiple ARS FACs. You can either use the global ARS codes, or provide ARS codes for a location.

For example, you might enter the access code 9 for ARS on the Feature Access Code (FAC) screen. You might then enter the ARS access code on a Locations screen as 1. When a user dials 1 from that location, the system routes the call with ARS. A user at that location cannot dial 9 to reach ARS.

Interactions for Multi-Location Dial Plan

This section provides information about how the Multi-Location Dial Plan feature interacts with other features in your system. Use this information to ensure that you receive the maximum benefits of the Multi-Location Dial Plan in any feature configuration.

Attendant

The feature states that it allows multiple attendant codes but not multiple attendant groups. You can use this feature to administer multiple attendant groups. However, you cannot use this feature to administer multiple attendant groups. You can have only one attendant group unless you have Attendant Partitioning. This feature provides a way to support multiple local centralized answering points (LCAPs). The LCAPs do not use attendant groups.

Attendant Vectoring

Attendant Vectoring, if enabled, takes precedence over any local attendant codes that are administered. The software uses call vectors to process calls to an attendant. Such calls are:

- Local attendant codes
- The attendant code on the Dial Plan Analysis Table screen
- The attendant access code on the Feature Access Code (FAC) screen

Automatic Circuit Assurance (ACA)

The **ACA Referral Destination** field on the System Features Parameters screen requires that an attendant group exists. This field also requires either:

- The attd administration on the Dial Plan Analysis Table screen, or
- Administration of the attendant access code on the Feature Access Code (FAC) screen

Automatic Wakeup

If a telephone has Automatic Wakeup requests pending when you run the **`change extension-station`** command, the system cancels the wakeup requests.

Call Forwarding

Any call forwarding information that is stored with an extension is lost when you use the **change extension-station** command. If the telephone that you change with the **change extension-station** command is a forwarded-to telephone, you must manually update the extension that uses the forwarded-to extension. If you do not manually update the extension, the system does not forward calls correctly.

Call Park

This feature does not support common shared extensions to park calls. Since common shared extensions are not assigned to physical telephones, the range of common shared extensions can be shared in all locations.

Crisis Alert

The **change extension-station** command does not update the **Originating Extension** field on the Crisis Alert System Parameters screen. You must manually update the **Originating Extension** field if you change the **originating extension** field.

Leave Word Calling (LWC)

The **Stations with System-wide Retrieval Permission for the Leave Word Calling Parameters** field on the System Features Parameters screen requires that an attendant group exists. This field also requires either:

- The attd administration on the Dial Plan Analysis Table screen, or
- Administration of the Attendant Access Code on the Feature Access Code (FAC) screen

Survivable Remote Server (Local Survivable Processor)

If you run the **change extension-station** command on the controller, but do not also save the translations to the Survivable Remote Server, the two system translations might be unsynchronized.

Use either of these following commands to save the translations to the Survivable Remote Server:

- The **save trans lsp** command locally saves the translations, and performs a filesync operation to all registered Survivable Remote Servers.
- The **save trans lsp** *n* command, where *n* is the IP address of a specific Survivable Remote Server, locally saves the translations, and performs a filesync operation to the specified Survivable Remote Server.

Night Service

This feature does not support location-based Night Service. Therefore, you might want to restrict calls to attendants who are local to the calling party. The attendant most likely speaks the same language as the caller. At night, instead of putting the entire system into Night Service, you might want an attendant to put only one location into Night Service.

To accomplish this, you can use hunt groups as attendant queues. Each hunt group can be put into Night Service separately, and have its own Night Service destination. You can also administer the Night Service destination by tenant, trunk group, and trunk group number.

Security Violations Notification

The referral destination fields on the Security-Related System Parameters screen requires that an attendant group exists. This field also requires either:

- The attd administration on the Dial Plan Analysis Table screen, or
- Administration of the attendant access code on the Feature Access Code (FAC) screen

The referral destination fields are:

- SVN Login Violation Notification Enabled
- SVN Remote Access Violation Notification Enabled
- SVN Authorization Code Violation Notification Enabled

Station Hunting

Changing a telephone extension with the **change extension-station** command maintains the hunting chain.

Survivable Remote EPN/WAN Spare Processor

If you run the **change extension-station** command in a configuration where a survivable remote processor exists, you must also run the command on the survivable processor. If you do not, the extensions that you changed on the server do not exist on the survivable remote when the remote processor takes control.

Uniform dial plan (UDP)

The **change extension-station** command does not update extensions that are in the Uniform Dial Plan Table screen. Avaya supports external system management tools that handles changes to the UDP table.

Chapter 127: Multiple Appearance Directory Number

Multiple Appearance Directory Number

To support migration of CS 1000 users to Avaya Aura®, the Multiple Appearance Directory Number (MADN) feature is now implemented in Communication Manager Release 8.0. The MADN feature was originally implemented on Nortel CS 1000. This feature is almost similar to the existing Communication Manager bridging feature.

As implemented on Nortel CS 1000, MADN has two flavors:

- Single call arrangement
- Multiple call arrangement
- The Single call arrangement feature operation is similar to the existing Communication Manager bridging feature with exclusion enabled. To enable single call arrangement like operation on Communication Manager, configure traditional per-call appearance bridges and enable exclusion by using Class of Service for the principal. For more information on bridging, see *Avaya Aura® Communication Manager Feature Description and Implementation*.
- The Multiple call arrangement feature defines a new form of bridge alerting that associates a bridge button to a principal extension, and not to a specific call appearance of a principal extension. A multiple call arrangement bridge allows an alerting bridge user to answer a call alerting on any call appearance of the principal, or even a call that does not alert at the principal because all principal call appearances are in use.
- Traditional per-call appearance bridge button: brdg-appr B:1 E:1000
- MAC per principal bridge button: brdg-appr B:`a` E:1000

By specifying the bridge button identifier (B) with the value `a`, this allows any call to principal 1000 to alert at this bridge button. A MAC bridge button may be used on any multi-call appearance DCP, H.323, or SIP station.

Traditional per-call appearance bridge buttons for station 1000 may exist on stations like 1001, 10002, 1003. While MAC bridge buttons for station 1000 may exist on stations like 2001, 2002, 2003. It is not valid for a station to have both per-call appearance and multiple call arrangement bridges for the same principal. Which means, station 1001 cannot have brdg-appr B:1 E:1000 and brdg-appr B:`a` E:1000.

Multiple call arrangement operation differs significantly on call answer. For an incoming call to a principal station, Communication Manager alerts all stations that have per-call appearance bridge matching a principal and for the particular call appearance. Additionally, Communication Manager alerts all stations that have an idle multiple call arrangement bridge for that principal.

If the call is answered on single call arrangement bridge, the principal and other per-call appearance bridges get a simulated bridge appearance. But, all multiple call arrangement bridge appearances are dropped.

However, if the call is answered at the multiple call arrangement bridge appearance, then:

- The principal gets dropped
- All the alerting single call arrangement bridge stations are dropped
- All the alerting multiple call arrangement bridge stations that did not answer the call gets dropped

Note:

You can administer up to 31 Multiple Appearance Directory Number (MADN) appearances for a principal station.

Related links

Screens for administering Multiple Appearance Directory Number on page 996
Assigning multiple call arrangement bridge to a Station on page 997

Screens for administering Multiple Appearance Directory Number

Screen name	Purpose	Fields
Station	Use a numeric B:1,2,3… value to specify a tradition per-call appearance bridged appearance or use B:a to specify a multiple call appearance bridged appearance	brdg-appr
	Enables a single burst of tone when a station bridges on to the principal's call.	Bridging Tone for This Extension?
cos	When enabled, allows a station to bridge onto a call which had exclusion activated.	Bridging Exclusion Override

Related links

Multiple Appearance Directory Number on page 995

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`.

Related links

Multiple Appearance Directory Number on page 995

Chapter 128: Multiple Call Handling

With the Multiple Call Handling feature, the diverted calls can be covered to the voicemail box of the principal party or the voicemail box of the last-forwarded-to party. Based on the Communication Manager configuration, the greeting of the administered party is played to the caller.

Related links

Detailed description of Multiple Call Handling on page 998

Detailed description of Multiple Call Handling

When Communication Manager receives a rerouted or a forwarded switched call, the call uses the coverage path of the diverted-to party. Communication Manager diverts the call due to one of the following settings on the principal party extension:

- Call Forwarding Unconditional (CFU)
- Call Forward Busy (CFB)
- Call Forward No Answer (CFNA)
- Send All Calls (SAC)
- Enhanced Call Forwarding All
- Enhanced Call Forwarding Busy
- Enhanced Call Forwarding No Answer

Related links

Multiple Call Handling on page 998

Multiple Call Handling administration

Screens for administering Multiple Call Handling

Screen name	Purpose	Field
SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING	Set the destination voice mail box for incoming QSIG diverted calls.	• QSIG/SIP Diverted Calls Follow Diverted to Party's Coverage Path • Diverted Party Identification

Related links

Multiple Call Handling on page 998

Administering Multiple Call Handling

Procedure

1. Type `change system-parameters coverage-forwarding` and press `Enter`.
2. On page 1 of the SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING screen, in the **QSIG/SIP Diverted Calls Follow Diverted to Party's Coverage Path?** field, type `y`. To disable the Multiple Call Handling feature, set the field to n.

   The system displays the **Diverted Party Identification** field.
3. In the **Diverted Party Identification** field, select one of the following:
   - Principal: To play the voice mail greeting of the principal party and save the voice message in the voice mail box of the principal party.
   - Last forwarded-to: To play the voice mail greeting of the last-forwarded party and save the voice message in the voice mail box of the last-forwarded party.
4. Save the changes.

Related links

Multiple Call Handling on page 998

Chapter 129: Multiple Level Precedence and Preemption

Users can activate the Multiple Level Precedence and Preemption (MLPP) feature to request priority processing of calls during critical situations.

Caution:

MLPP is currently designed to meet regulations use by federal, state, or local government agencies. MLPP is not currently designed for use in commercial enterprise environments. Activation of this feature in any other type of network environment can result in unexpected or unwanted feature operations.

Detailed description of Multiple Level Precedence and Preemption

The Multiple Level Precedence and Preemption feature is available with Communication Manager Release 2.0 (V12) or later.

The media servers and gateways that are referenced in this document support MLPP, the Joint Interoperability Test Command (JITC) has certified only the following servers:

- S8300D
- S8300E
- HP DL360 G7
- Dell R610

Multiple Level Precedence and Preemption supports the following capabilities:

- Precedence Calling
- Announcements for Precedence Calling
- Precedence Call Waiting
- Precedence Routing
- Dual Homing

- End Office Access Line Hunting
- Preemption
- Line Load Control
- Worldwide Numbering and Dialing Plan

Precedence Calling

Users can use Precedence Calling to select a level of priority for each call on a call-by-call basis. The need of the user and the importance of the call is the basis for the priority. The call can receive a priority routing whether the call is local or international.

From Communication Manager Release 7.1 onwards, you can dial precedence calls to SIP endpoints and SIP endpoints can initiate any precedence calls.

Precedence levels

Users can access five levels of precedence:

- Flash Override, which is the highest precedence level
- Flash
- Immediate
- Priority
- Routine, which is the default and the lowest precedence level

If a user does not specify a precedence level, the system treats dialed calls as Routine level precedence calls.

The administrator assigns a maximum precedence level to each telephone user. The more important or higher in rank of the user, the higher the precedence level. Users cannot originate calls at precedence levels that are higher than the maximum administered level. Non-MLPP calls are treated as Routine level precedence calls.

For example, General Davis has a maximum precedence level of Flash assigned to his telephone. Without intervention, everyday calls are treated at the Routine level. One day, a crisis occurs at a military installation, and the general must make an emergency call to his field commanders over the Defense Switched Network (DSN). General Davis can use the Precedence Calling feature to raise the level of his call to Priority, Immediate, or Flash. When he places this call, the communication server gives the call priority handling, and the call is sent over the DSN access line.

Format for dialed digits with Precedence Calling

The following table shows the format for Precedence Calling dialed digits:

Access digits		Address digits		
FAC	**Precedence digit**	**Area code**	**Office code**	**Extension**
A	P	[NXX]	NXX	XXXX

Where:

A is the Feature Access Code (FAC) for Precedence Calling

P is any digit from 0 to 4 (digits from 5 to 9 can also be used)

X is any digit from 0 to 9

N is any digit from 2 to 9

Brackets [ ] indicate optional digits

Access digits for Precedence Calling

The access digits are comprised of the FAC for the Precedence Calling feature, plus a Precedence Level digit. The single-digit code used for the Precedence Level digit is administered as shown on Assigning Precedence Calling system parameters.

The default Precedence Level digits are:

Digit	Precedence Level
0	Flash Override
1	Flash
2	Immediate
3	Priority
4	Routine

Address digits for Precedence Calling

The address digits are the 7-digit or the 10-digit telephone number.

Precedence calls above the Routine level use special precedence ringback tones for the calling party, and a special ringing pattern for the called party.

On a Branch Gateway supported by S8300E, or a duplicated server, the gateway processor generates precedence calling tones.

- The ringback tone is a 1.65-second burst of mixed 440-Hz and 480-Hz tone, and then 0.35 seconds of silence. This tone repeats until the call is answered, the caller hangs up, or the Precedence Call Timeout occurs. For more information, see Assigning Precedence Calling system parameters.
- The ringing pattern for precedence calls is the same three-burst ring that is used with Priority Calling.

Precendence Calling diversion

When a precedence call to a telephone goes unanswered, the system attempts to connect the caller to a backup point as follows:

1. The call is diverted to the attendant console.
2. If the console is in Night Service or no console is administered, the call is diverted to a night telephone.

3. If no console or night telephone is administered, the call can be diverted to a user-defined telephone. This user-defined telephone is called the Remote Attendant Route String.

   The Attendant Diversion Timing controls how long that this type of call rings before the system routes the call to the Remote Attendant Route String. The Remote Attendant Route String is any valid telephone number on the network, and is usually a backup answering position for the remote attendant console. The Remote Attendant Route String does not raise the precedence level of the call.
4. If the Remote Attendant Route String is undefined and there is no attendant console or night telephone is administered, the call rings until the call is answered or abandoned.

These Precedence Calling diversion scenarios have variations for DSN calls, non-DSN calls, and local calls:

DSN Calls: If an outgoing precedence call over a DSN trunk is unanswered after an administrable period of time, the system routes the call to the:

- Attendant console or night telephone on the remote communication server
- Remote Attendant Route String

The administrable period of time is the Precedence Call Timeout on the remote communication server.

Non-DSN Calls: If an outgoing precedence call over a non-DSN trunk is not answered after an administrable period of time, the system routes the call to:

- A local attendant console or night telephone on the local communication server
- The Remote Attendant Route String

The administrable period of time is the Attendant Diversion Timing on the local communication server.

Local calls: If a local, intraswitch precedence call is unanswered after an administrable period of time, the system routes the call to:

- A local attendant console
- A night telephone
- The Remote Attendant Route String

Note:

For a precedence call that diverts to a night telephone or to a Remote Attendant Route String, the number must be administered in the Precedence Routing digit-conversion tables. For more information, see Assigning digit conversion and Assigning Precedence Calling system parameters.

The administrable period of time is the Precedence Call Timeout on the remote communication server.

When calls are redirected, a Call Purpose Indicator is displayed on the attendant console and on display telephone sets to indicate the precedence level of the call. The following indicators are provided:

- FO - Flash Override
- FL - Flash
- IM - Immediate
- PR - Priority

Routine precedence calls do not have a Call Purpose Indicator.

When callers attempt to use a precedence level that is higher than the authorized level, the caller hears the “Unauthorized precedence level attempted” recording. If an announcement is unassigned, the caller hears intercept tone.

The following table shows how precedence calls are processed depending on the precedence level and the administered maximum precedence level of the caller:

Maximum precedence level of the user	Precedence level of the call	Call treatment
Flash Override	Flash Override	Call completes normally
Flash Override	Flash	Call completes normally
Flash Override	Immediate	Call completes normally
Flash Override	Priority	Call completes normally
Flash Override	Routine	Call completes normally
Flash	Flash Override	Recorded announcement or intercept tone
Flash	Flash	Call completes normally
Flash	Immediate	Call completes normally
Flash	Priority	Call completes normally
Flash	Routine	Call completes normally
Immediate	Flash Override	Recorded announcement or intercept tone
Immediate	Flash	Recorded announcement or intercept tone
Immediate	Immediate	Call completes normally
Immediate	Priority	Call completes normally
Immediate	Routine	Call completes normally
Priority	Flash Override	Recorded announcement or intercept tone
Priority	Flash	Recorded announcement or intercept tone
Priority	Immediate	Recorded announcement or intercept tone
Priority	Priority	Call completes normally
Priority	Routine	Call completes normally
Routine	Flash Override	Recorded announcement or intercept tone
Routine	Flash	Recorded announcement or intercept tone

Table continues…

Maximum precedence level of the user	Precedence level of the call	Call treatment
Routine	Immediate	Recorded announcement or intercept tone
Routine	Priority	Recorded announcement or intercept tone
Routine	Routine	Call completes normally

Related links

Assigning digit conversion for Precedence Routing on page 1029
Assigning Precedence Calling system parameters on page 1019

How service domains influence preemption and precedence

You define MLPP service domains at two levels:

- On the Class of Restriction screen, where you then assign the COR to a telephone of a user
- On the Multiple Level Precedence & Preemption Parameters screen, which applies to all resources on the server

The system uses the service domain to determine whether the system applies the preemption or precedence level of the caller to potentially preempt a routine call or another call of lower precedence. If an existing call has a different service domain than the service domain of the call that attempts a preemption, preemption is disallowed, regardless of the preemption levels of the two calls.

The two levels of service domain influence preemption and precedence capabilities in different ways, depending on which of the following resources the server recognizes as carrying the call:

- Intraswitch routing to another telephone on the same server
- Incoming ISDN-PRI trunks for a call that originates from another server on the network
- Incoming non-ISDN-PRI trunks for a call that originates from another server on the network

MLPP Station-to-station calls on the same server

If a user makes an MLPP call to another user whose telephone resides on the same server, and if the called telephone is busy with an existing call, the server uses the following process to determine whether to grant precedence to the new call:

1. The server assigns the existing call to the service domain that is defined in the Class of Restriction (COR) of the caller.
2. The server checks the COR of the new caller to define the service domain of the new call.
3. The server matches the service domain of the new call with the service domain of the existing call.
4. If the service domains match, the server matches the precedence level of the existing call with the precedence level of the new call. If the new call has a higher level, the new call preempts the existing call.

If the service domains do not match, then the server gives the new call an announcement that says the MLPP call cannot be completed. The figure on page 1006 shows this process.

MLPP Station-to-station calls on the same server scenario

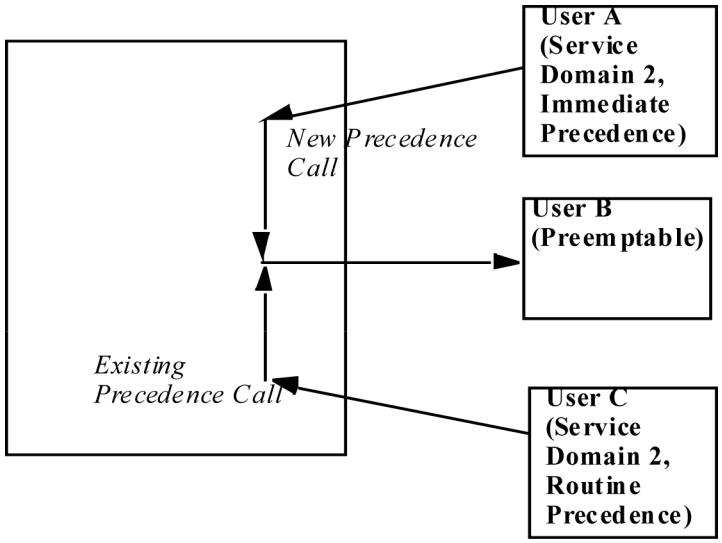


Figure 23: Station-to-station calls on the same server

In the figure on page 1006, the server uses the service domains and the precedence levels to treat calls as follows:

1. User C makes a routine call to user B and is still connected. The server checks the service domain of the COR of user C, and assigns service domain 2 to the call.
2. User A makes an immediate precedence call to user B. The server checks the service domain of the COR of user A, and assigns service domain 2 to the call.
3. The server matches the service domain of user C with the service domain of user A.
4. Because the calls are in the same service domain, and because user A used a higher precedence level than user C, the server allows user A to preempt the call of user C.

Precedence calls to destinations over ISDN-PRI trunks

If:

- A user makes an MLPP call to another user whose telephone resides on a different MLPP server, and
- The call arrives at the server of the called user over an ISDN-PRI trunk, and
- The called telephone is busy with an existing call.

The destination MLPP server uses the following process to determine whether to grant precedence to the new call:

1. The server assigns the existing call to the service domain that is defined either in the COR of the caller, or by the system service domain.

2. The server checks the COR of the new caller to define the service domain of the new call.
3. The server matches the service domain of the new call with the service domain of the existing call.
4. If the service domains match, the server matches the precedence level of the existing call with the precedence level of the new call. If the new call has a higher level, the new call preempts the existing call.

   If the service domains do not match, the server gives the new call an announcement that says that the MLPP call cannot be completed. The figure on page 1007 shows this process.

Precedence calls to destinations over ISDN-PRI trunks scenario

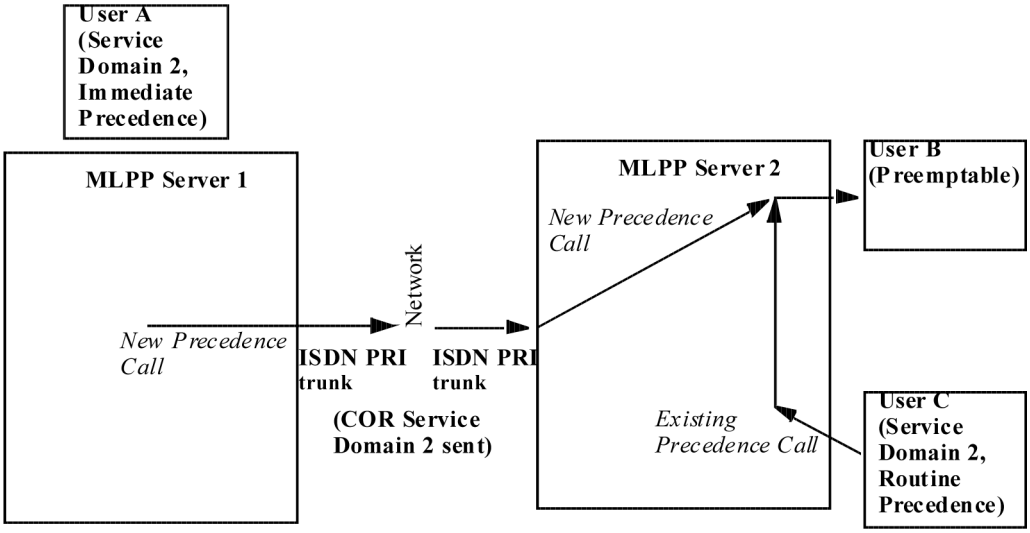


Figure 24: Precedence calls to destinations over ISDN-PRI trunks

In the figure on page 1007, the destination server, MLPP Server 2, uses the service domains and precedence levels to treat calls as follows:

1. User C makes a routine call to user B and is still connected. The server checks the service domain of the COR of user C, and assigns service domain 2 to the call.
2. User A, who is on MLPP Server 1, makes a precedence call to user B. Server 2 checks the service domain on the incoming ISDN call and finds service domain 2, which is defined in the COR of user A on Server 1. Server 2 assigns service domain 2 to the call.
3. The server matches the service domain of user C with the service domain of user A.
4. Because the calls are in the same service domain, and because user A used a higher precedence level than user C, the server allows user A to preempt user C.

Precedence calls to destinations over non-ISDN-PRI trunks

If:

- A user makes an MLPP call to another user whose telephone resides on a different MLPP server, and

- The call arrives at the server of the called user over a non-ISDN-PRI trunk, and
- The called telephone is busy with an existing call,

The destination server uses the following process to determine whether to grant precedence to the new call:

1. The server assigns the existing call to the service domain that is defined either in the COR of the caller, or by its own system service domain.
2. The server checks its own system service domain to define the service domain of the new call.
3. The server matches the service domain of the new call with the service domain of the existing call.
4. If the service domains match, the server matches the precedence level of the existing call with the precedence level of the new call. If the new call has a higher level, the new call preempts the existing call.

   If the service domains do not match, then the server gives the new call an announcement that says that the MLPP call cannot be completed. The figure on page 1008 shows this process.

Precedence calls to destinations over non-ISDN-PRI trunks scenario

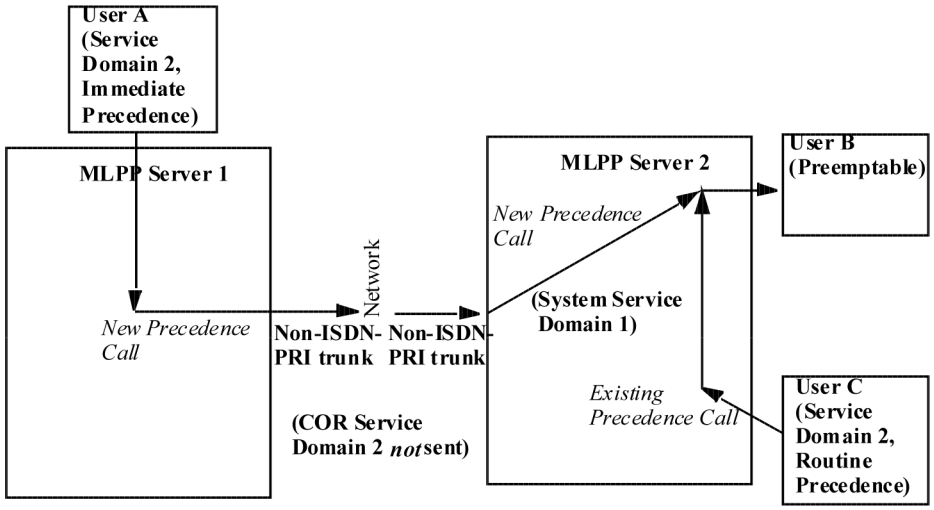


Figure 25: Precedence calls to destinations over non-ISDN-PRI trunks

In the figure on page 1008, the system uses the service domains and precedence levels to treat calls as follows:

1. User C makes a routine call to user B and is still connected. The server checks the service domain of the COR of user C, and assigns service domain 2 to the call.
2. User A, who is on MLPP Server 1, makes a precedence call to user B. Because the call from user A arrives at MLPP Server 2 on a non-ISDN-PRI trunk, Server 2 does not receive the service domain identifier of user A. Server 2 assigns the system service domain 1 to the call.

3. The server matches the service domain of user C with the service domain of user A.
4. Because the calls of users A and C are not in the same service domain, calls from user A receive an announcement that says that the MLPP call cannot be completed.

Hot Line Number for Precedence Calling

A hot line is an extension that the system automatically dials when you pick up the receiver. On a single-line telephone, assign a hot line destination. Use a system, a group, or a personal list that is administered to the hot line destination.

The hot line number must include,

- Precedence Calling FAC
- Precedence Level digit, see Precedence Calling on page 1001
- Destination telephone number

For example, when the system dials 807208451111, the system processes the call as a Flash Override precedence voice call to extension 720-845-1111, where

- 8 is the Precedence Calling FAC
- 0 is the Precedence Level digit for Flash Override
- 720-845-1111 is the destination telephone number

The following procedure explains how to administer number 807208451111 as a hot line destination number. To administer a hot line destination number, you must first set up a group list that contains the hot line destination number. Then you must set up the hot line destination number that references the group list.

Announcements for Precedence Calling

In certain situations, precedence calls are blocked because of unavailable resources or improper use. The MLPP feature requires special announcements, for calls higher than Routine precedence, to notify users when Precedence Calling is denied, or when service is unavailable.

The announcements that MLPP uses include:

Blocked precedence call

This announcement plays when the system attempts to preempt an existing call with a call that has a precedence level higher than Routine precedence that is also equal to or lower than the precedence level of the current call. If an announcement extension is unassigned, the caller hears reorder tone (fast busy).

Unauthorized precedence level attempted

This announcement plays when a caller attempts to place a precedence call with a precedence level that is higher than the level that is authorized by the COR of the caller. If an announcement extension is unassigned, the caller hears intercept tone.

Service-interruption-prevented call completion

This announcement plays when a service interruption prevents a precedence call from being completed. If an announcement extension is unassigned, the caller hears reorder tone.

Busy, not equipped for Preemption or Precedence Call Waiting

This announcement plays when a precedence call is placed to a busy line, and the line does not have Precedence Call Waiting or cannot be preempted. If an announcement extension is unassigned, the caller hears reorder tone.

Vacant code

This announcement plays when a precedence call is placed to an unassigned extension. If an announcement extension is unassigned, the caller hears reorder tone.

If a caller is using Routine precedence and the call cannot be completed for any of these reasons, the caller hears busy tone.

No Circuits Available

This announcement plays when an outgoing call is blocked due to the Destination Code Control (DCC) feature.

Attendant Queue

This announcement plays when an incoming precedence call above Routine precedence level is placed in the attendant waiting queue.

Leaving DSN Network

This announcement plays when a call egresses Communication Manager over a trunk facility that is not assigned for DSN. The announcement is played to the caller and the call then proceeds to its destination. If the announcement extension is unassigned then the call proceeds to its destination without any notification to the caller.

Precedence Call Waiting

After the system routes a precedence call, the called party might already be busy on another call. With Precedence Call Waiting, the caller can “camp on” to the line of the called party, and wait for the called party to answer the call. The caller hears a special ringback tone, and the called party hears a call waiting tone. Depending on the type of telephone, the called party:

- Can put the current call on hold and answer the incoming call, or
- Can disconnect the current call to answer the incoming call

Precedence Routing

When precedence calls are destined for other switches in a network, the Precedence Routing feature routes the calls. The Precedence Routing feature routes calls based on the:

- Destination number
- Precedence level
- Time of day

These routing criteria are administrable and can be changed as required. Two related features are Dual Homing and End Office Access Line Hunting.

Dual Homing

A user can activate Dual Homing to dial a telephone number and have the system route the call to its destination over alternate facilities if the initial route is unavailable. This operation is transparent to the user, and no special dialing is required.

Dual Homing uses the Precedence Routing feature to provide alternate routing to nodes on a DSN. If a call fails to complete over the first trunk access line, the call is rerouted over a different trunk access line. This process can continue for any number of alternate routes.

If the call fails to complete by the time the call gets to the last trunk access line, the system routes the call to either:

- Busy tone, or
- The Blocked precedence call recorded announcement, see Announcements for Precedence Calling.

For example, a user dials a DSN number, such as 345-8854. Using Precedence Routing, you administer the system to route all calls that begin with the digits “345”:

1. First over trunk group 20
2. Then over trunk group 21
3. Finally over trunk group 22

If all trunks in trunk group 20 are busy, the system next checks for idle trunks in trunk group 21, and finally in trunk group 22. If all trunks in all three trunk groups are busy, the system routes the call to fast busy tone or to a recorded announcement.

For a more detailed description of the available routing options, see Precedence Routing on page 1010.

MLPP End Office Access Line Hunting

The End Office Access Line Hunting feature automatically hunts for an idle trunk over end office access lines. This feature hunts for an idle trunk based on the precedence level of the call. The search occurs over either a preemptable trunk group or a nonpreemptable trunk group.

For calls that are higher than Routine precedence, the system hunts for an idle trunk in a preemptable trunk group. The following steps describe the hunting algorithm:

1. If the system finds an idle trunk, the system provides precedence ringing.
2. If the system does not find an idle trunk, the system reexamines a preemptable trunk group on a preemptive search. The system preempts an active call that is of the lowest available precedence level.
3. The system hunts for an idle trunk in a nonpreemptable trunk group. If the system finds an idle trunk, the system provides precedence ringing.
4. If the system cannot find a trunk, the call is routed to the Blocked precedence call recorded announcement, see Announcements for Precedence Calling. If announcements are not recorded or administered, the caller hears reorder tone.

For calls that are Routine precedence, the system hunts for an idle trunk in a nonpreemptable trunk group and attempts to connect the call. If the system does not find an available trunk, the caller hears busy tone. For more information about preemptable and nonpreemptable trunks, see Preemption.

Preemption with Precedence Routing

Preemption works with Precedence Routing to further extend the call routing capabilities of MLPP. Preemption actually disconnects an existing, lower-priority call to complete a more important precedence call. Even non-MLPP calls are treated as Routine level precedence calls, and can be preempted.

When preemption occurs, the callers on the existing call hear a tone that indicates that the system is about to preempt the call. The callers have 3 seconds to end the call before the system automatically disconnects the call. After the system disconnects the call, the system places the new call over the preempted facility.

MLPP Line Load Control

Line Load Control (LLC) is a feature that restricts a predefined set of telephone users from originating calls during a crisis or an emergency. LLC systematically reduces the number of telephones that can originate calls during high-traffic periods. This situation is sometimes called a “lockdown.” When the lockdown situation passes, the LLC restriction levels can be reduced or removed completely.

Users are assigned to a Line Load Control level based on the relative importance of the position of the user within the organization. When an emergency occurs, the administrator manually activates the LLC feature to restrict calls by users with positions that are of lower importance. When the emergency is over, the administrator manually disables the LLC feature.

For example, if a security emergency occurs, telephone users who are responsible for managing the crisis are unrestricted from originating calls. Other telephone users, for example, users in the accounting department, are restricted. When the crisis is over, the administrator returns the system to normal operation.

The LLC feature can be controlled at four levels. These levels determine what telephones, based on the Class of Restriction (COR), are restricted from originating calls. This feature does not restrict incoming calls, or calls that originate from an attendant console or a night telephone.

The four levels are as follows:

Level	Definition
0	The LLC feature is inactive, that is, no restrictions exist. This is the default setting.
2	Restrict telephones with a COR that is assigned to LLC levels 2, 3, and 4.
3	Restrict telephones with a COR that is assigned to LLC levels 3 and 4.
4	Restrict telephones with a COR that is assigned to LLC level 4.

System level 1 is an invalid value. The LLC feature cannot restrict telephones with a COR that is assigned to LLC level 1 from originating calls.

When LLC is activated, the system restricts all telephones with a COR at that LLC level and below from originating any calls. If a restricted telephone is already active on a call when the restriction is activated, the call is neither interrupted nor disconnected. The telephone becomes restricted only after the user hangs up from the active call.

When the need for LLC has passed, the administrator can change the LLC to a less-restrictive level, or completely deactivate the feature.

The following table shows how the LLC feature can be used.

Extension	COR	LLC Level
5300	11	0
5350	12	2
2540	13	3
3300	14	4
2635	14	4

For this example, the LLC is at Level 0, and extension 2635 is active on a call.

1. Because of high telephone traffic, the system administrator changes the LLC to level 3.

   Extensions 2635, 2540, and 3300 cannot originate calls because the assigned COR LLC level for these extensions is equal to or less than the system LLC level.

   The active call on extension 2635 is undisturbed. As soon as extension 2635 disconnects, this extension cannot originate calls.

   Extensions 5300 and 5350 can originate calls because the assigned COR LLC level of these extensions is higher than the system LLC level.

2. Call traffic is still too high, so the system administrator changes the LLC to level 2.

   Now extension 5350, in addition to extensions 2635, 2540, and 3300, cannot originate new calls. Extension 5300 can still originate new calls.

3. Call traffic subsides. The system administrator changes the LLC back to level 0.

   All extensions can now originate calls.

MLPP Worldwide Numbering and Dialing Plan

The Worldwide Numbering and Dialing Plan (WNDP) feature is compatible with the standard numbering system that the Defense Communications Agency (DCA) established. WNDP is a dialing system that is used in a Defense Switched Network (DSN). WNDP is similar to Precedence Calling, but the pattern of digits that users dial is different.

The following table shows the format of the dialed digits:

Access digits		Address digits		
FAC	**Route code**	**Area code**	**Office code**	**Extension**
A	[[1]X]	[NXX]	NXX	XXXX

Where:

A is the 2-digit WNDP FAC for the precedence level

1 is a Route Code setup digit.

X is any digit from 0 to 9

N is any digit from 2 to 9

Brackets [ ] indicate optional digits

Worldwide Numbering and Dialing Plan Feature Access Code

The Feature Access Code (FAC) is the set of two-digit WNDP FACs. Each precedence level uses a unique FAC.

- Flash Override - 90
- Flash - 91
- Immediate - 92
- Priority - 93
- Routine - 94

Worldwide Numbering and Dialing Plan Route Code

After dialing the FAC, the user has the option to dial a Route Code. The Route Code is a 2-digit DSN code that consists of a Route Code Setup digit and the Route Code digit. The Route Code informs the communication server of special routing or termination requirements. The Route Code is limited to the DSN. The Route Code determines whether a call uses data-grade or voice-grade trunking. The Route Code also indicates whether the dialed number is a Federal Telephone System (FTS) or a Continental US (CONUS) commercial number.

If you do not require special call features, and you want to use the default value 0, you do not have to use the Route Code. If you want to use a value other than the default value 0, you must use the Route Code.

- The first digit of the Route Code is the Route Code Setup digit. The Route Code Setup digit is the number 1. The Route Code Setup digit indicates that the next digit gives instructions to the network for specialized routing. If a Route Code is dialed, the Route Code Setup digit is deleted, and the second digit is saved.
- The second digit of the Route Code is the Route Code digit. Valid entries are:

  0 - Voice call (the default value)

  1 - Circuit switched data call

  2 - Satellite avoidance call

  3 - (reserved)

  4 - (reserved)

  5 - Hotline voice-grade call

6 - Hotline data-grade call

7 - (reserved)

8 - (reserved)

9 - (reserved)

The Route Code digit becomes part of the dialed number, and can be used for route selection by the Precedence Routing translations. With Precedence Routing, digit strings to be modified before outpulsing. This capability modifies the Route Code as needed by the terminating trunk group. If a Route Code digit is not dialed, the system inserts the default Route Code Digit of 0 as defined on the Multiple Level Precedence & Preemption Parameters screen. The default Route Digit routes the calls over the voice network, not the data network.

Address Digits with the Worldwide Numbering and Dialing Plan

The Address Digits are the 7-digit or the 10-digit DSN number.

The following table shows the format of the outpulsed digits:

Precedence digit	Route code	Address digits		
		Area code	Office code	Extension
P	[[1]X]	[NXX]	NXX	XXXX

Use the Precedence Routing functionality to administer the digit outpulsing. For more information, see Precedence Routing. With Precedence Routing, you can have flexible routing of dialed numbers and the ability to modify the digits outpulsed digits as needed. For example, you can administer Precedence Routing to outpulse no Route Digit, only the Route Digit, or the number 1 and the Route Digit. The digits sent to Precedence Routing are of the form:

PRXXX...

Where:

P is the Precedence Digit

R is the Route Code (if WNDP is active)

XXX... are the Address Digits

If a particular route requires the Route Code of the form 1X, you can use the digit modification translations for the route to insert the number 1. If the route does not require the Route Digit, the digit modification can be translated to delete the Route Digit. The digit modification translations insert a Default Route Digit if the Default Route Digit is not dialed.

Hot Line Number for WNDP

A hot line is an extension that the system automatically dials when you pick up the receiver. On a single-line telephone, assign a hot line destination. Use a system, a group, or a personal list that is administered to the hot line destination.

The hot line number must include,

- WNDP Dialing 2-digit FAC for the precedence level that you want.
- As an option, you can also include the number 1 as the Route Code setup digit.

  For more information, see Worldwide Numbering and Dialing Plan. If you do not use a Route Code setup digit, the system uses the default digit 0.

  If you use the Route Code setup digit 1, you must use a routing digit. The next number in the sequence is the routing digit. For example, 5 is a hot line voice call, and 6 is a hot line data call. For more information, see Worldwide Numbering and Dialing Plan.
- Destination telephone number.

For example, when the system dials 90157208451111, the system processes the call as a Flash Override WNDP voice call to extension 720-845-1111, where

- 90 is the two-digit WNDP dialing FAC indicating Flash Override.
- 1 is the optional Route Code setup digit.
- 5 is the routing digit that indicates a voice hot line call.
- 720-845-1111 is the destination telephone number.

The following procedure explains how to administer number 90157208451111 as a hot line destination number. To administer a hot line destination number, you must first set up a group list that contains the hot line destination number. Then you must set up the hot line destination number that references the group list.

For information on setting up a group list and assigning the hot line destination number, see Setting up a group list and Assigning the Hot Line Destination Number.

In this example, you need to administer the following fields:

- Set the **Dial Code** field on the Abbreviated Dialing List screen to the 90157208451111 hot line destination number.
- Assign the hot line destination number to the extension 90157208451111.

Multiple Level Precedence and Preemption administration

The following tasks are part of the administration process for the Multiple Level Precedence and Preemption feature:

- Precedence Calling administration
- Precedence Calling announcement administration
- Precedence Call Waiting administration
- Precedence Routing administration
- Dual Homing administration

- End Office Access Line Hunting administration
- Preemption administration
- Line Load Control administration
- Worldwide Numbering and Dialing Plan administration

Related links

Worldwide Numbering and Dialing Plan administration on page 1033
Line Load Control administration on page 1030
Preemption administration on page 1029
End Office Access Line Hunting administration on page 1029
Dual Homing administration on page 1029
Precedence Routing administration on page 1026
Precedence Call Waiting administration on page 1025
Precedence Calling announcement administration on page 1023
Precedence Calling administration on page 1019

Preparing to administer Multiple Level Precedence and Preemption

Procedure

1. Enter `display system-parameters customer-options`.
2. Ensure that the **G3 Version** field is set to V17 or later.
3. Click **Next** until you see the **Multiple Level Precedence and Preemption** field.
4. Ensure that the **Multiple Level Precedence and Preemption** field is set to y.

   Note:

   If the **Multiple Level Precedence and Preemption** field is set to n or the **G3 Version** field is not set to V12, go to the Avaya Support website at http://support.avaya.com to open a service request.

5. Press `Enter` to exit the screen.

Screens for administering Multiple Level Precedence and Preemption

Screen name	Purpose	Fields
Optional Features	Ensure that you have Communication Manager version 2.0 (V17) or later.	G3 Version
	Ensure that the MLPP feature is on.	Multiple Level Precedence & Preemption

Table continues…

Screen name	Purpose	Fields
Feature Access Code (FAC)	Set up FACs for users to activate the MLPP features.	• Precedence Calling Access Code • All the fields in the **WNDP Precedence Access Codes** area
	Set up a FAC for users to originate a Precedence Call Waiting call from an H.323 or a SIP deskphone.	CAS Remote Hold/ Answer Hold-Unhold Access Code
Multiple Level Precedence & Preemption Parameters	Set up the system parameters for MLPP.	All
Class of Restriction	• Apply administration settings to all objects that share the same COR number. • Restrict the types of calls that a user can make and receive.	• Maximum Precedence Level • Preemptable • MLPP Service Domain • Lineload Control
Trunk Features	Assign a trunk group as a DSN termination telephone.	DSN Term
	For DS1 and analog TIE trunks only, indicate if the system sends or receives the precedence level as digits (rotary pulses) or as dual-tone multifrequency (DTMF) signals (touchtones).	• Precedence Incoming • Precedence Outgoing
Station	Activate or deactivate Precedence Call Waiting for a telephone.	Precedence Call Waiting
	Assign a telephone as a hot line telephone for a precedence call or a WNDP call.	All the fields in the **Hot Line Destination** area
Abbreviated Dialing List	Set up the dialing list and specific dialed string to be used with a hot line telephone.	All
Console Parameters	Assign attendant queue priorities.	All the fields in the **Queue Priorities** area
Announcements/Audio Sources	Assign extensions for Precedence Calling announcements.	All
Precedence Routing Digit Analysis Table	Administer how the system analyzes Precedence Routing digits.	All

Table continues…

Screen name	Purpose	Fields
Pattern Number	Administer how the system handles route patterns for outgoing Precedence calls.	All
Precedence Routing Digit Conversion Table	Administer how the system takes digits of incoming calls, and converts the digits to local telephone numbers.	All

Precedence Calling administration

The following tasks are part of the administration process for the Precedence Calling feature:

- Assigning an MLPP Feature Access Code
- Assigning Precedence Calling system parameters
- Assigning a maximum precedence level
- Assigning trunks for Precedence Calling
- Setting up a group list
- Assigning the hot line destination number
- Assigning attendant queue priorities for Precedence Calling

Assigning an MLPP Feature Access Code

Procedure

1. Enter `change feature-access-codes`.
2. Click **Next** until you see the **MLPP Features** area.
3. In the **Precedence Calling Access Code** field, enter values in the following fields:
   - **Flash Override Access Code**
   - **Flash Access Code**
   - **Immediate Access Code**
   - **Priority Access Code**
   - **Routine Access Code**
4. Press `Enter` to save your changes.
5. Ensure that you notify all users about the assigned FAC.

Assigning Precedence Calling system parameters

Procedure

1. Enter `change system-parameters mlpp`.
2. In the **Precedence Calling-Dialed Digit Assignment** fields, make any necessary changes.

Caution:

Avaya recommends that you do not change the default Precedence Calling dialed digits unless you are coordinating this change with other companion networks in your system. If the Precedence Calling digits do not match across networks, the system does not properly process the calls. Each of the Precedence Calling digits must be different. You cannot use the same digit for two different precedence levels.

- Flash Override. 0 to 9 or blank (the default is 0)
- Flash. 0 to 9 or blank (the default is 1)
- Immediate. 0 to 9 or blank (the default is 2)
- Priority. 0 to 9 or blank (the default is 3)
- Routine. 0 to 9 or blank (the default is 4)
- Attendant Diversion Timing. 10 to 99 seconds or blank (the default is blank)
- Remote Attendant Route String. 1 to 24 numeric digits or blank (the default is blank). When you administer this string, use address digits only. Do not use FACs. For more information, see Precedence Calling diversion scenarios.
- Precedence Call Timeout. 10 to 60 seconds (the default is 30)
- Default Service Domain. 0 to 16777215. This number defines the system service domain, and must be unique within a switching network. The system uses the system service domain to determine eligibility for precedence calling when interswitch precedence calls over non-ISDN trunks occur.

3. Press `Enter` to save your changes.

Related links

Precendence Calling diversion on page 1002

Assigning a maximum precedence level

About this task

Maximum precedence levels are assigned to Classes of Restriction (COR).

Procedure

1. Enter `change cor n`, where *n* is the number of a specific COR.
2. Click **Next** until you see the **Maximum Precedence Level** and **MLPP Service Domain** fields.
3. In the **Maximum Precedence Level** field, type one of the following values:
   - fo (Flash Override)
   - fl (Flash)
   - im (Immediate)
   - pr (Priority)

- ro (Routine, the default value)

4. In the **MLPP Service Domain** field, type a number from 0 to 16777215.

   This number defines the service domain for users and trunks to which this particular COR is assigned. The system uses the service domain to create a group of MLPP users or facilities, within which precedence calls can be made.

5. Press `Enter` to save your changes.

Assigning trunks for Precedence Calling

Procedure

1. Enter `add trunk-group n`, where *n* is the number of a trunk group.
2. Click **Next** until you see the **DSN Term** field.
3. Use the **DSN Term** field to identify the trunk group as a DSN termination telephone.

   The default is n.

   - The system displays the **Precedence Incoming** and **Precedence Outgoing** fields, if:
     - You type `y` in the **DSN Term** field, and
     - The value in the **Group Type** field on page 1 of this screen is tie.

       These two fields define whether the precedence level for dual-tone multifrequency (DTMF) or tone trunks is received or sent as digits (rotary pulses) or as DTMF signals (touchtones).
   - The system does not display the **Precedence Incoming** and **Precedence Outgoing** fields, if:
     - You enter `n` in the **DSN Term** field, or
     - You enter `y` in the **DSN Term** field, and the value in the **Group Type** field on page 1 of this screen is isdn, or
     - You enter `y` in the **DSN Term** field, and the value in the **Group Type** field on page 1 of this screen is tie, and the value in both the **Outgoing Dial Type** and **Incoming Dial Type** fields on page 1 of this screen is mf2/6.

4. Press `Enter` to save your changes.

Setting up a group list

Procedure

1. Enter `add abbreviated-dialing group next`.
2. Write down the Group List number that the system assigns to this Abbreviated Dialing List.

   You use this Group List number when you set up the hot line destination number.

3. In the **Dial Code** field, type the dial code that is associated with the hot line destination number. In this example, that number is 807208451111.

4. Press `Enter` to save your changes.

Assigning the Hot Line Destination Number

Procedure

1. Enter `add station 807208451111`.
2. In the **Type** field, type the model of analog telephone, such as 2500.
3. Type information in the other fields that the system requires to add this new extension.
4. Click **Next** until you see the **Hot Line Destination** area.
5. In the **Abbreviated Dialing List Number (From above 1, 2, or 3)** field, type the Group List number that contains your hot line destination number.

   This is the Group List number that you wrote down from the previous procedure.
6. Press `Enter` to save your changes.

Assigning attendant queue priorities for Precedence Calling

Procedure

1. Enter `change console-parameters`.
2. Click **Next** until you see the **MLPP Precedence Call** area.
3. Use the **MLPP Precedence Call** area to assign attendant queue priorities for precedence calls and nonprecedence calls.

   This process determines how the system queues calls to the attendant console. Depending on the priority that you want for processing calls, you can change the system defaults. The defaults are:

   - Flash Override: 2
   - Flash: 3
   - Immediate: 4
   - Priority: 5

   Important:

   By default, emergency access calls receive a higher priority processing than MLPP Precedence Calls. You can change the order of priority, but be careful when designating emergency calls to an equal or lower priority. Call types with equal priority enter the queue on a first-in, first-out basis.

   Routine precedence calls are treated as normal calls and use the same queue priorities as nonemergency and nonMLPP calls.
4. Press `Enter` to save your changes.

Precedence Calling announcement administration

The following tasks are part of the administration process for the Precedence Call announcement feature:

- Adding extensions for Precedence Calling announcements
- Assigning announcement types for Precedence Calling
- Recording announcements for Precedence Calling
- Deleting announcements for Precedence Calling
- How to save Precedence Calling announcements

This feature uses the standard recorded announcements feature in Communication Manager. For more information about administering recorded announcements, see the Announcements feature description.

Adding extensions for Precedence Calling announcements

Procedure

1. Enter `change announcements`.
2. Assign extensions for the different MLPP recorded announcements.

   The extensions that you use for recorded announcements must already be administered in your dial plan. The extensions cannot be used for any other purpose, such as individual telephones or directory numbers.
3. Press `Enter` to save your changes.

Assigning announcement types for Precedence Calling

About this task

After you add the announcement extensions, you must designate the extensions to use for each of the announcement types. This administration is unique to the Announcements for Precedence Calling feature.

Procedure

1. Enter `change system-paramters mlpp`.
2. Match the extensions that you set on the Announcements/Audio Sources screen with the five announcements.
3. Press `Enter` to save your changes.

Recording announcements for Precedence Calling

About this task

Use the following procedures to record and test the announcements. You must record the announcements from the attendant console or from a telephone that has console permissions.

Procedure

1. Go off-hook and dial the FAC for the Announcement feature.
2. Dial the extension of the announcement that you want to record.

   If an announcement session is already in progress, or if a save or a restore command is in progress, you hear reorder tone. Try again later.
3. Press `1` and record the announcement after the tone.

   Note:

   If the announcement already exists and is marked as “protected” in the Announcements screen, you hear intercept tone.

   The following wording is suggested for each of the five announcements:

   - Blocked precedence call: Equal or higher precedence calls prevented completion of your call. Please hang up and try again later.
   - Unauthorized precedence level attempted: The precedence level that you requested is not authorized for your line. Please use an authorized precedence level, or ask your operator for assistance.
   - Service interruption prevented call completion: A service interruption prevented the completion of your call. Please wait 30 seconds and try again. In case of emergency, call your operator.
   - Busy, not equipped for Preemption or Precedence Call Waiting: The number that you dialed is busy and not equipped for Preemption or Precedence Call Waiting.
   - Vacant code announcement: Your call cannot be completed as dialed. Please consult your directory and call again, or ask your operator for assistance.
4. Disconnect when you finish recording each message.

   Note:

   The system records the sound of the receiver returning to the telephone cradle. To disconnect gently, either press Drop, or quietly press the switchhook with your finger.
5. Wait for 15 seconds, and then dial the extension of the announcement that you just recorded.

   Listen to the recording.

   - If you need to record the message again, repeat this procedure.
   - If the message is satisfactory, disconnect and repeat this procedure to record the other announcements.

Deleting announcements for Precedence Calling

Procedure

1. Go off-hook and dial the FAC for the Announcement feature.

2. Dial the extension of the announcement that you want to delete.
3. Press `3`.

   The system deletes the announcement.
4. Disconnect the call.
5. Type `change announcements` to delete the announcement extension.

   For more information, see Adding extensions.

How to save Precedence Calling announcements

The announcements on virtual VAL announcements on the S8300D and S8300E servers are not saved through system administration. You can back up the announcement to a personal computer. For procedures to back up the announcements, see the Announcements feature description.

Precedence Call Waiting administration

The following tasks are part of the administration process for the Precedence Call Waiting feature:

- Enabling Precedence Call Waiting for a telephone
- Setting the Precedence Call timeout
- Assigning Precedence Call Waiting FACs

Enabling Precedence Call Waiting for a telephone

About this task

Enable or disable the Precedence Call Waiting feature for each telephone on your system. The default assignment for each telephone is y (enabled).

Procedure

1. Enter `change station` *n*, where *n* is the telephone extension that you want to enable or disable.
2. Click **Next** until you see the **Precedence Call Waiting** field.
3. In the **Precedence Call Waiting** field, perform one of the following actions:
   - Type `y` to enable the Precedence Call Waiting feature.
   - Type `n` to disable the Precedence Call Waiting feature.
4. Press `Enter` to save your changes.

Setting the Precedence Call timeout

Procedure

1. Enter `change system-paramters mlpp`.
2. In the **Precedence Call Timeout (sec)** field, set the number of seconds before a precedence call is timed out.

The valid values are 10 to 60 seconds, with a default of 30 seconds.

3. In the **ISDN Precedence Call Timeout (sec)** field, set the number of seconds before an ISDN precedence call is timed out.

   The valid values are 10 to 60 seconds, with a default of 30 seconds.

4. Press `Enter` to save your changes.

Assigning Precedence Call Waiting FACs

About this task

For users of single-line analog telephones, you must assign a Feature Access Code (FAC) to answer a Precedence Call Waiting call.

Procedure

1. Enter `change feature-access-codes`.
2. In the **CAS Remote Hold/Answer Hold-Unhold Access Code** field, assign a FAC that matches your dial plan.
3. Press `Enter` to save your changes.
4. Ensure that you notify all users about the assigned FAC.

Precedence Routing administration

This section contains procedures for administering Precedence Routing when the local and the remote DSN nodes are both Avaya communication servers. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to:

- Trunk administration when you connect local DS1 trunks to a DSN node that uses an Avaya communication server
- Administration procedures when you connect local DS1 trunks to a DSN node that uses a Nortel switch
- Administration procedures when you connect local DS1 trunks to a DSN node that uses a Siemens switch

Assigning digit analysis for Precedence Routing

About this task

Digit analysis determines what routes are used for outgoing calls based on the digits dialed.

Procedure

1. Enter `change precedence-routing analysis n`, where *n* is the digit or digits being analyzed.

   Except for the **Preempt Method** field, the digit analysis administration is the same as Automatic Route Selection (ARS) and Automatic Alternate Routing (AAR) digit analysis.

2. Format the **Dialed String** field for routing DSN numbers:
   - For non-WNDP dialing, enter the precedence digit and the address digits. The precedence digit is usually a number from 0 to 4.
   - For WNDP dialing, enter the precedence digit, the route code, and the address digits. The precedence digit is usually a number from 0 to 4.

     An *x* in the digit string is a wildcard that matches any single digit.

     The **Preempt Method** field has two possible values, group and route. The default preemption is group.

     With group preemption:

     a. The system checks the first trunk group in the route pattern to determine if any trunks are idle.

        If the system finds an idle trunk, the system connects the call.

     b. If no trunks are idle, the system checks the same trunk group to determine if any trunks are preemptable.

        If the system finds a preemptable trunk, the system preempts the current call and connects the new call.

     c. If no trunks are idle or preemptable, the system checks the next trunk group to determine if any trunks are idle.

        If the system finds an idle trunk, the system connects the call.

     d. If no trunks are idle, the system checks the same trunk group to determine if any trunks are preemptable.

        If the system finds a preemptable trunk, the system preempts the current call and connects the new call.

     e. If the system does not find an idle trunk or a preemptable trunk within the Precedence Call Timeout interval, the caller hears either the Blocked Precedence recorded announcement or reorder tone.

        For more information, see Announcements for Precedence Calling. Calls with Routine precedence cannot preempt any other calls. If a call with Routine precedence does not find an idle trunk, the caller receives busy tone.

Assigning digit analysis for Precedence Routing example

About this task

For example, trunk groups 1, 2, and 3 are set up as follows:

- Trunk group 1 has two trunk members active with Flash and Flash Override precedence calls.
- Trunk group 2 has two trunk members active with Immediate and Priority precedence calls.
- Trunk group 3 has two trunk members, both of which are idle.

A user makes a new call with the Flash precedence level. The system processes the call as follows:

1. The system checks trunk group 1, and does not find an idle trunk. The system then checks trunk group 1, and does not find a preemptable active call.
2. The system checks trunk group 2, and does not find an idle trunk. The system then checks trunk group 2, and finds two preemptable active calls. The system preempts the first trunk member that the system finds with a lower precedence level. In this example, the new Flash call preempts the active Immediate precedence call.
3. The system never checks trunk group 3, even though trunk group 3 has idle trunks.

With route preemption:

1. The system checks each trunk group in the route pattern to determine if any trunks are idle. If the system finds an idle trunk, the call is connected.
2. If the system does not find an idle trunk, the system checks each trunk group in the route pattern to determine if any trunks are preemptable. If the system finds a preemptable trunk, the system preempts the current call and connects the new call.
3. If the system does not find an idle trunk or a preemptable trunk within the Precedence Call Timeout interval, the caller hears either the Blocked Precedence recorded announcement or reorder tone. For more information, see Announcements for Precedence Calling. Calls with Routine precedence cannot preempt any other calls. If a call with Routine precedence does not find an idle trunk, the caller receives busy tone.

For example, trunk groups 1, 2, and 3 are set up as follows:

- Trunk group 1 has two trunk members active with Flash and Flash Override precedence calls.
- Trunk group 2 has two trunk members active with Immediate and Priority precedence calls.
- Trunk group 3 has two trunk members, both of which are idle.

A user makes a new call with the Flash precedence level. The system processes the call as follows:

1. The system checks trunk group 1, and does not find an idle trunk.
2. The system checks trunk group 2, and does not find an idle trunk.
3. The system checks trunk group 1, and finds an idle trunk. The system completes the new Flash call using the first idle trunk.
4. Select `Enter` to save your changes.

Assigning route patterns for Precedence Routing

About this task

The system uses these routing patterns for outgoing calls.

Procedure

1. Enter `change route-pattern` *n*, where *n* is a route pattern from the Precedence Routing Digit Analysis Table screen.

2. For DSN trunks that have the **Precedence Mode Outgoing** field set for DTMF, you must delete one digit.

   If you do not delete one digit, the system sends the precedence level digit twice.

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

Assigning digit conversion for Precedence Routing

About this task

Digit conversion takes digits that were dialed on incoming calls, and converts the digits to local telephone numbers. These local numbers usually are extensions.

Procedure

1. Enter `change precedence-routing digit-conversion`.
2. Format the **Matching Pattern** field for routing DSN numbers:
   - For non-WNDP dialing, enter the precedence digit and the address digits. The precedence digit is usually a number from 0 to 4.
   - For WNDP dialing, enter the precedence digit, the route code, and the address digits. The precedence digit is usually a number from 0 to 4.

     An *x* in the digit string is a wildcard that matches any single digit.
3. In the **Net** fields, type `ext` or `pre`.
   - ext stands for extension, and uses ARS tables or AAR tables to route the call.
   - pre stands for precedence routing, and uses the Precedence Analysis Tables to route the call.
4. Select `Enter` to save your changes.

Dual Homing administration

You administer Dual Homing when you administer the Precedence Routing feature. For more information, see Precedence Routing.

End Office Access Line Hunting administration

You administer End Office Access Line Hunting when you administer the Precedence Routing feature. For more information, see Precedence Routing.

Preemption administration

The following tasks are part of the administration process for the preemption:

- Assigning Preemption to a COR
- Trunks for Preemption administration
- Precedence Call timeout administration

Assigning Preemption to a COR

Procedure

1. Enter `change cor n`, where *n* is the number of a specific COR.
2. Click **Next** until you see the **Preemptable** field.
3. In the **Preemptable** field, define whether extensions or trunks that you assign to this COR can be preempted.

   The default value is y.
4. Select `Enter` to save your changes.

Trunks for Preemption administration

For the Preemption feature, enabling a trunk as a DSN termination telephone guarantees that the trunk can accept the Preemption signaling over the DSN.

The following task is the part of administration process of Trunks for Preemption feature:

- Assigning trunks

Precedence Call timeout administration

The following task is part of the administration process for Precedence Call timeout feature:

- Assigning Precedence Calling system parameters

Line Load Control administration

Line Load Control (LLC) is assigned on a system-wide basis and on a COR basis.

The following tasks are part of the administration process for Line Load Control feature:

- Assigning the LLC level for the system
- Assigning the LLC to a COR

Assigning the LLC level for the system

Procedure

1. Enter `change system-parameters mlpp`.
2. Set the LLC level for the system.

   In the **Line Load Control Restriction Level** field, type one of the following options:

   - 0 - The LLC feature is inactive. There are no restrictions. This is the default value.
   - 2 - Restrict extensions with a COR that is assigned to LLC level 2, 3, or 4.
   - 3 - Restrict extensions with a COR that is assigned to LLC level 3 or 4.
   - 4 - Restrict extensions with a COR that is assigned to LLC level 4.
3. Select **Enter** to save your changes.

Configuring Line Load Control (LLC) Restriction for the location

About this task

Line Load Control (LLC) is a feature that restricts a predefined set of telephone users from originating calls during a crisis or an emergency. LLC systematically reduces the number of telephones that can originate calls during high-traffic periods. This situation is sometimes called as a lockdown. When the lockdown situation passes, the LLC restriction levels can be reduced or removed completely.

Procedure

1. Enter `change location-parameters x`
2. Click next until you see **Line Load Control Restriction** field.
3. Enter the values in the followig fields:
   - Restriction Level

     to specify the line load control level for COR, please see below table

Valid Entry	Usage
0	Feature not active (no restrictions). This is the default.
2	Restrict stations with a COR assigned to LLC levels 2, 3, and 4.
3	Restrict stations with a COR assigned to LLC levels 3, and 4.
4	Restrict stations with a COR assigned to LLC level 4.

   - Feature Access Code Authentication Required

   For more information about Feature Access Code Authentication Required, seeFeature Access Code Authentication Required: N (Default) on page 1032 and Feature Access Code Authentication Required: y on page 1032.

Configuring Line Load Restriction Control Per Location

Procedure

1. Enter `change feature-access-code`.
2. Click Next until you see the **LINE LOAD RESTRICTION CONTROL PER LOCATION** field.
3. In **Autherization Code** field, enter one of the following feature access code.

   Refer the table below to know more information about the Feature Access Code.

Level of Restriction	Feature Access Code
0	*190
2	*192
3	*193
4	*194

   By entering Feature access code, Communication Manager will enable Line Load Control Restriction Level.

Assigning the LLC level from the Phone

Feature Access Code Authentication Required: N (Default)

Procedure

1. Dail Feature Access Code from phone.
2. After successfully dialing a Feature Access Code, you will hear a confirmation code or a denial code.

   In case of failure, log a denial event by giving relevant information

Feature Access Code Authentication Required: y

Procedure

1. Dial Feature Access Code from phone.

   After successfully dialing a Feature Access Code, you will be prompted to enter an Authorization Code.
2. Enter Authorization code after hearing a dial tone.
3. After successful entry of Authorization code, you will hear a confirmation code or a denial code.

   Upon the successful entry of an Authorization code, the you will be granted permission to change the Line Load Control (LLC) Restriction Level per each Location, and LLC level is modified on stations location.

   In case of failure, a denial event will be logged, providing relevant information.

   Note:

   After successful enablement of LLC, an entry will be added with the following details:

   - Previous and Current LLC Restriction Level
   - The Extension Number, Location and LLC level of the user
   - The date and time of the activation

   To activate the **Line Load Control** feature, you need to enable both the **Multiple Level Precedence & Preemption** and **Multiple Location** features.

Assigning the LLC to a COR

Procedure

1. Enter `change cor n`, where *n* is the number of a specific COR.
2. Click **Next** until you see the **Line Load Control** field.
3. Set the LLC level for each COR.

   In the **Line Load Control** field, type one of the following options:

   - 1 - LLC Level 1. The COR cannot be restricted by LLC. This is the default value.

- 2 - LLC Level 2
- 3 - LLC Level 3
- 4 - LLC Level 4

4. Press `Enter` to save your changes.

Worldwide Numbering and Dialing Plan administration

The following tasks are the part of the administration process for worldwide numbering and dialing plan feature:

- Assigning WNDP system parameters
- Assigning WNDP Feature Access Codes
- Assigning a hot line number for WNDP

Assigning WNDP system parameters

Procedure

1. Enter `change system-parameters mlpp`.
2. In the **Worldwide Numbering Dial Plan Active**, type either `y` or `n`.
3. In the **Default Route Digit**, type a valid digit.

   The system displays this field when the **Worldwide Numbering Dial Plan Active** field is enabled.
4. In the **WNDP Emergency 911 Route String**, type a numeric digit.

   Valid entries for this field can be a trunk access code (TAC), the AAR or the ARS access code, a WNDP access code, or an extension. The extension might be, for example, the firehouse at a base that handles emergency calls. If you use a WNDP access code, use the access code for the lowest precedence calling level in the system.

   For more information, see Interactions for Multiple Level Precedence and Preemption.
5. Select **Enter** to save your changes.

Related links

Interactions for Multiple Level Precedence and Preemption on page 1036

Assigning WNDP Feature Access Codes

About this task

Administer the WNDP precedence FACs only when you use WNDP dialing. Do not administer the WNDP precedence FACs when you use precedence dialing.

Procedure

1. Enter `change feature-access-codes`.
2. Click **Next** until you see the **WNDP Precedence Access Codes** area.

Note:

You must also define a value in the **Precedence Calling Access Code** field, even when you use WNDP dialing. Use the Precedence Calling FAC when you administer Precedence Routing trunks. For more information, see Assigning an MLPP Feature Access Code.

3. In the **WNDP Precedence Access Codes** area, type a 2-digit FAC that conforms to your dial plan in each field.

   Each FAC must begin with the number 9.

4. Select **Enter** to save your changes.
5. Ensure that you notify all users about the assigned FACs.

Assigning a hot line number for WNDP

Procedure

1. Set up a group list.
2. Assign the hot line destination number.

WNDP attendant queue priorities administration

The following task is part of administration process for WNDP attendant queue priorities feature:

- Assigning attendant queue priorities

Considerations for Multiple Level Precedence and Preemption

This section provides information about how the Multiple Level Precedence and Preemption feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Multiple Level Precedence and Preemption under all conditions.

Considerations for Announcements for Precedence Calling

When you use the announcement capabilities on G250 Branch Gateway, G350 Branch Gateway, G430 Branch Gateway, G450 Branch Gateway, or G700 Gateway to record announcements on the following servers:

- S8300E
- HP DL360 G7
- Dell R610

Note:

- From Avaya Aura® Release 10.1, HP ProLiant DL360p G8 (CSR2), HP ProLiant DL360 G9 (CSR3), Dell™ PowerEdge™ R620 (CSR2), Dell™ PowerEdge™ R630 (CSR3), and Avaya Solutions Platform 120 servers are not supported.

  However, in Release 10.1, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.x, and S8300E can be upgraded to Avaya Solutions Platform S8300 R5.1.x.

- From Avaya Aura® Release 10.1, Appliance Virtualization Platform is not available for deploying or upgrading the Avaya Aura® applications. To upgrade the Avaya Aura® applications, migrate the Appliance Virtualization Platform to Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.x.

You can also use existing analog announcement equipment with the MLPP features.

Considerations for Precedence Call Waiting

You can assign Precedence Call Waiting to all models of telephones, including IP hardphones and softphones.

Considerations for Precedence Routing

The routing that you administer with Precedence Routing uses the same capacity tables as the ARS feature. These tables include patterns and analysis tables. You can view the real-time capacity usage with the **`change precedence-routing analysis`** command. The **Percent Full** field displays how much of the available capacity is used for routing information.

H.323 IP trunks do not support data calls that use any type of modem or data module. Do not administer H.323 IP trunks for users who make data calls over trunk facilities. H.323 IP trunks can be used for voice calls.

Considerations for Preemption

The call progress tones for Preemption consist of a fixed tone and a pattern. You cannot change the call progress tones by typing the **`change system-parameters country-options`** command.

Considerations for Line Load Control

When a system reload occurs, the LLC system-level settings revert to the default factory setting. The default factory setting is LLC level 0, which indicates no restrictions. Normal telecommunications service is restored after a system reload.

The LLC COR settings, however, are saved in translations. The settings do not revert to the factory defaults if the settings were saved in translations.

Considerations for Worldwide Numbering and Dialing Plan

The Route Control Digit of the Worldwide Numbering and Dialing Plan (WNDP) feature is unavailable as part of the MLPP feature set.

The Route Control Digit of WNDP is different than the Route Code digit.

Users must dial any destination telephone number that starts with the number 1, such as extension 1500, as follows: 1, the Route Code digit, then the destination number. For example, dial 1x1500, where x is the Route Code digit.

H.323 IP trunks do not support data calls. Do not administer H.323 IP trunks for users that make data calls over trunk facilities. H.323 IP trunks can be used for voice calls.

Interactions for Multiple Level Precedence and Preemption

This section provides information about how the Multiple Level Precedence and Preemption feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Multiple Level Precedence and Preemption in any feature configuration.

Note:

Dual Registration and Multiple Device Access are not supported together for a user.

Interactions for Precedence Calling

Attendant Vectoring

Attendant Vectoring uses the Call Vectoring feature to provide flexible routing of attendant-seeking calls. When the system accesses an attendant VDN, the call can be answered by the attendant, routed to an announcement, or routed to the voice mailbox of the assigned night station. This process reduces the chance of precedence calls remaining in the attendant queue, specifically where the attendant has not answered all calls in the queue, and the console is placed in night mode. Attendant Vectoring can be purchased as a standalone feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to Attendant Vectoring.

For more information about Attendant Vectoring, see *DEFINITY ECS Call Vectoring/EAS Guide*.

Call Coverage

Calls above Routine precedence do not follow administered coverage paths. The calls ring until the Timeout for Precedence Calls expires, and the call goes to a console or a night telephone. If the called party is on an active call and Preemption is enabled, the call is preempted.

Call Detail Recording (CDR)

No separate CDR field is supplied for the precedence level of a call. **No separate CDR** field creates an incompatibility between current call accounting software and the new call record format. With the current call record format, you can examine the call record for the Precedence Calling FAC to determine the precedence level of a call. If the call is a precedence call, the first

digit of the number that was dialed indicates the precedence level of the call. If WNDP is active, you need to examine only the FAC because the precedence level is implied from the FAC. The CDR feature does not record the precedence level for a station-to-station call.

CDR can be administered to record either the dialed digits or the outpulsed digits. In the case of Precedence Routing, the outpulsed digits can be different from the dialed digits. When you view CDR records, remember that the precedence level digit might not be recorded.

Conference

When two calls are merged during a conference, the precedence level of a call is set to the highest active precedence level.

Hunting

When you administer a hunt group with preemption, set the **Maximum Preemption Level** field and the **Preemptable** field in the Class of Restriction screen. The hunt group Group Type must use circular or ucd-mia queuing, and the ACD, the Queue, and the Vector fields must be set to n.

Night Service

When the attendant console goes into Night Service, users can answer precedence calls from a night telephone, a night or a day/night console, or the Trunk Answer Any Station (TAAS) feature. If calls are in the queue when the attendant console goes into Night Service, those queued calls are diverted to a night or a day/night console or TAAS, based on the attendant queue priorities. For more information, see “Assigning attendant queue priorities” in the “Administering” section.

Preemption

When a precedence call attempts to preempt an existing call, call progress tones, or the “blocked precedence call” announcement, indicates why the system did not complete the call.

The following table shows how the system processes precedence calls based on the precedence level of the call and the precedence level of the preempted trunk.

Precedence level of the call	Precedence level of the DSN trunk call that is being preempted	Call treatment
Flash Override	Flash Override	Recorded announcement or busy tone
Flash	Flash Override	Recorded announcement or busy tone
Immediate	Flash Override	Recorded announcement or busy tone
Priority	Flash Override	Recorded announcement or busy tone
Routine	Flash Override	Busy tone
Flash Override	Flash	Call completes normally
Flash	Flash	Recorded announcement or busy tone
Immediate	Flash	Recorded announcement or busy tone
Priority	Flash	Recorded announcement or busy tone
Routine	Flash	Busy tone
Flash Override	Immediate	Call completes normally
Flash	Immediate	Call completes normally

Table continues…

Precedence level of the call	Precedence level of the DSN trunk call that is being preempted	Call treatment
Immediate	Immediate	Recorded announcement or busy tone
Priority	Immediate	Recorded announcement or busy tone
Routine	Immediate	Busy tone
Flash Override	Priority	Call completes normally
Flash	Priority	Call completes normally
Immediate	Priority	Call completes normally
Priority	Priority	Recorded announcement or busy tone
Routine	Priority	Busy tone
Flash Override	Routine	Call completes normally
Flash	Routine	Call completes normally
Immediate	Routine	Call completes normally
Priority	Routine	Call completes normally
Routine	Routine	Busy tone

Restrict Last Appearance

If the Restrict Last Appearance telephone option is enabled, and only one idle call appearance is available on the telephone when a precedence call is made to that telephone, callers who use Routine precedence hear busy tone. Callers who use any other precedence level connect to the restricted last call appearance.

If the Restrict Last Appearance telephone option is inactive, and only one idle call appearance is available on the telephone when a precedence call is made to that telephone, callers using any precedence level connect to the last call appearance.

Send All Calls

Calls above Routine precedence do not follow administered coverage paths. Calls ring until the Timeout for Precedence Calls expires, and then calls go to an attendant console or a night telephone.

Transfer

When two calls are merged during a transfer, the precedence level of a call is set to the highest active precedence level.

Worldwide Numbering and Dialing Plan (WNDP)

When WNDP is enabled, users must dial a FAC for the precedence level that the users want to use. Users cannot use the Precedence Calling FAC. In addition, the Route Code function and the implied precedence level are provided.

When WNDP is disabled, users must dial the Precedence Calling FAC, and then the precedence level, a number between 0 and 4. The WNDP FACs can be administered, but cannot be used.

Interactions for Precedence Call Waiting

Attendant Console

Precedence Call Waiting calls from attendant consoles or telephones with console permissions are not supported. Calls from an attendant console cannot camp onto a call with Precedence Call Waiting. The attendant console user hears a recorded announcement.

Automatic Callback

If the Automatic Callback feature is activated and Precedence Call Waiting is attempted, the caller hears a recorded announcement.

Call Forwarding

An extension can have Precedence Call Waiting and Call Forwarding active at the same time. If the user is active on a call and another call comes in, the called party hears the Precedence Call Waiting tone. The call is forwarded after the timeout. Any other calls that arrive during the timeout period go immediately to the forwarded telephone.

Call Pickup

If a member of a pickup group who is active on a call receives Precedence Call Waiting, other members of the pickup group cannot pick up the call.

Call Waiting

- For a Routine Precedence Call, a user who is on an active call hears the standard Call Waiting tone.
- Precedence Call Waiting is denied if the called party already has one call currently waiting in queue.

Data Privacy

Precedence Call Waiting cannot be applied to a line with Data Privacy.

Data Restriction

Precedence Call Waiting cannot be applied to a line with Data Restriction.

Line Load Control (LLC)

If the LLC feature restricts a telephone, that user must hang up to answer a Precedence Call Waiting call.

Preemption

Regardless of how you administer Precedence Call Waiting, calls with a higher level of precedence always preempt calls with a lower level of precedence.

Tenant Service Partitioning

Timeout redirection does not occur. Tenant Service Partitioning calls continue to ring at the called extension.

Interactions for Precedence Routing

General

With Precedence Routing, calls with a precedence higher than Routine to terminate to:

- Trunks
- Telephones
- Attendant consoles
- Hunt groups
- Recorded announcements

  Precedence Routing calls cannot terminate at Vector Directory Numbers (VDNs) or Terminating Extension Groups (TEGs).

Call Detail Recording (CDR)

No separate CDR field is supplied for the precedence level of a call. **No separate CDR** field creates an incompatibility between current call accounting software and the new call record format. With the current call record format, you can examine the call record for the Precedence Calling FAC to determine the precedence level of a call. If the call is a precedence call, the first digit of the number that was dialed indicates the precedence level of the call. If WNDP is active, you need to examine only the FAC because the precedence level is implied from the FAC. The CDR feature does not record the precedence level for a station-to-station call.

The **cca-id** field is the new CDR field related to MLPP. This field does not provide any information on precedence level of calls but shows the CCA ID of Communication Manager. The information displayed in the field comes from the MLPP form field: **Call Control Agent Identification (CCA-ID)**.

CDR can be administered to record either the dialed digits or the outpulsed digits. In the case of Precedence Routing, the outpulsed digits can be different from the dialed digits. When you view CDR records, remember that the precedence level digit might not be recorded.

Chained Call Forwarding

Precedence routing works with call forwarding (one hop), however it is not supported with chained call forwarding (multiple hops).

Shortcut Dialing

When you use the Shortcut Dialing feature over DSN trunks, the system uses the Precedence Routing analysis tables to administer the incoming Shortcut Dialing digit analysis. The system does not use the ARS analysis tables.

Traveling Class Marks TCM)

Precedence Routing passes all TCM information over DSN and non-DSN trunks.

Interactions for Preemption

General

Calls can be preempted that terminate at:

- Trunks
- Telephones
- Attendant consoles
- Nonqueued hunt groups
- Vector Directory Numbers (VDNs)

  Since with Precedence Routing, precedence calls cannot be terminate at queued hunt groups or terminating extension groups (TEGs), other calls to these facilities cannot be preempted.

Adjunct Switch Applications Interface (ASAI)

ASAI is notified if a call is preempted and disconnected from the current call.

Communication Manager Messaging system

The Communication Manager Messaging system is notified if a call is preempted and disconnected from the current call.

Call Detail Recording (CDR)

CDR has two records for a preempted call. CDR has a record of the original call, and a record of the new call after the preemption.

Call Management System (CMS)

CMS is notified if a call is preempted and disconnected from the current call.

Call Coverage

A call that the system redirects to a coverage point cannot be preempted.

Call Pickup

A call that uses Call Pickup cannot be preempted.

Code Calling Access

A call that uses Code Calling Access cannot be preempted.

Emergency Calls

Emergency calls can be preempted for H.323 deskphones. But you can administer Communication Manager to block the preemption of emergency calls.

For network preemption, emergency calls are not preempted irrespective of the flag setting on Communication Manager.

Avaya Interactive Voice Response (IVR) system

The system notifies the IVR system if the system preempts and disconnects a call from the current call.

Group Paging

A call that is part of a group page cannot be preempted.

Loudspeaker Paging

A call that uses Loudspeaker Paging cannot be preempted.

Malicious Call Trace

A call that uses Malicious Call Trace cannot be preempted.

Modem Pooling

A call that uses a modem pool cannot be preempted.

OPTIM OPS

An OPTIM OPS trunk can be preempted.

Personal central office line (PCOL)

A call that uses PCOL cannot be preempted.

Precedence Calling

When a precedence call attempts to preempt an existing call, call progress tones or the “blocked precedence call” announcement indicates why the system did not complete the call.

The following table shows how precedence calls are processed, depending on the precedence level of the call and the precedence level of the preempted trunk.

Precedence level of the call	Precedence level of the DSN trunk call that is being preempted	Call treatment
Flash Override	Flash Override	Recorded announcement or busy tone
Flash	Flash Override	Recorded announcement or busy tone
Immediate	Flash Override	Recorded announcement or busy tone
Priority	Flash Override	Recorded announcement or busy tone
Routine	Flash Override	Busy tone
Flash Override	Flash	Call completes normally
Flash	Flash	Recorded announcement or busy tone
Immediate	Flash	Recorded announcement or busy tone
Priority	Flash	Recorded announcement or busy tone
Routine	Flash	Busy tone
Flash Override	Immediate	Call completes normally
Flash	Immediate	Call completes normally
Immediate	Immediate	Recorded announcement or busy tone
Priority	Immediate	Recorded announcement or busy tone
Routine	Immediate	Busy tone

Table continues…

Precedence level of the call	Precedence level of the DSN trunk call that is being preempted	Call treatment
Flash Override	Priority	Call completes normally
Flash	Priority	Call completes normally
Immediate	Priority	Call completes normally
Priority	Priority	Recorded announcement or busy tone
Routine	Priority	Busy tone
Flash Override	Routine	Call completes normally
Flash	Routine	Call completes normally
Immediate	Routine	Call completes normally
Priority	Routine	Call completes normally
Routine	Routine	Busy tone

Precedence Call Waiting

Regardless of how you administer Precedence Call Waiting, calls with a higher level of precedence always preempt calls with a lower level of precedence.

Radio Paging

You cannot preempt a call that uses Radio Paging.

Recorded Announcements

You cannot preempt a call that is connected to a recorded announcement.

Secondary Extension

You cannot preempt a call that uses a secondary extension.

Transient calls

You can preempt calls, either ringing or on hold, that are in a transient mode.

Interactions for Line Load Control

General

Since the Line Load Control (LLC) feature restricts telephones from originating calls, features that require dial tone or a new call appearance for activation are unavailable when LLC is restricting the telephone. Some of those features include:

- Call Forwarding
- Call Pickup
- Conference
- Transfer

  You can still activate features that use buttons, where dial tone is not required. Some of those features include:

- Send All Calls
- Inspect
- Integrated Directory

Bridged Call Appearance

The LLC feature restricts originating new calls from all call appearances on a telephone, including bridged appearances. A telephone that is restricted by the LLC feature, and that has a bridged appearance of an extension of an unrestricted telephone, can bridge onto an active call, but cannot originate a new call through that bridged extension.

A telephone that is not restricted by the LLC feature, and that has a bridged appearance of an extension whose telephone is restricted, can originate a new call through that bridged extension.

Call Park

A user on a call becomes restricted by the LLC feature. The user can park the call, but cannot retrieve the call until the LLC restriction is removed. Another user that is not currently restricted by the LLC feature can retrieve the call.

Call Waiting

A user whose telephone is restricted by the LLC feature must hang up to answer a Call Waiting call. The LLC feature does not restrict incoming calls.

Hold

Telephones that are restricted by the LLC feature, and that are on an active call, can place a call on hold and later retrieve the call that is on hold.

Precedence Call Waiting

A user whose telephone is restricted by the LLC feature must hang up to answer a Precedence Call Waiting call.

Interactions for Worldwide Numbering and Dialing Plan

Emergency 911 Calling

If WNDP dialing is administered to use the digits 91 as a FAC, this FAC conflicts with dialing 911 to reach an emergency service agency. If a user dials 911 with WNDP enabled, the call does not go through to the emergency service agency because the system is waiting for more digits after dialing 91.

To work around this interaction, you can take all or any the following actions:

- Instruct users to first dial the ARS FAC and then dial 911. For example, if the ARS FAC is 8, a user can dial 8911. This option works for any emergency number, such as 999 in the United Kingdom.
- Instruct users to dial the assigned WNDP FAC followed by 911. For example, if one of the WNDP FACs is 92, a user can dial 92911. This option works for any emergency number, such as 999 in the United Kingdom.
- Administer a WNDP Emergency 911 Route String. This route string is outpulsed when a user dials either 911 and waits for the interdigit timeout, or dials 911 and then presses #. This dialing option works only when the WNDP Flash FAC is 91.

If the telephone that you use for an emergency call does not have adequate calling permissions, the emergency call does not go through. This situation can happen in the following conditions:

- The Facility Restriction Level (FRL) of the telephone is not high enough.
- The precedence calling level of the telephone is not high enough.
- The telephone cannot use a higher precedence level for the call.
- No trunk facilities are available, and the precedence level of the call is not high enough to preempt another call.
- The hop limit is exceeded when call is routed over tandem trunks.

Hunting

When you administer a hunt group with preemption, set the **Maximum Preemption Level** field and the **Preemptable** field in the Class of Restriction screen. The hunt group Group Type must use **circular** or **ucd-mia queuing**, and the **ACD**, the **Queue**, and the **Vector** fields must be set to n.

Precedence Calling

When WNDP is enabled, users must dial a FAC for the precedence level that the users want to use. Users cannot use the Precedence Calling FAC. In addition, the Route Code function and the implied precedence level are provided.

When WNDP is disabled, users must dial the Precedence Calling FAC, and then the precedence level, a number between 0 and 4. The WNDP FACs can be administered, but cannot be used.

Chapter 130: Multiple signaling groups in one SIP trunk group

By assigning members from multiple SIP signaling groups to one SIP trunk group, you can directly connect a SIP-integrated Avaya Aura® Messaging system with multiple Messaging Application Servers (MASs) to Communication Manager. Using this connection, Communication Manager can handle the load balancing between MAS devices.

Detailed description of multiple signaling groups in one SIP trunk group

To assign members from more than one signaling group to one SIP trunk group, you must first set up the signaling groups. After setting up the signaling groups you must assign members from more than one signaling group to one SIP trunk group. You can have one signaling group per MAS.

For example, if you have three MASs within the Messaging system, you must configure three signaling groups, one for each MAS. A single SIP trunk group can then be created with members from the three signaling groups.

Multiple signaling groups in one SIP trunk group administration

The following tasks are part of the administration process for assigning members from more than one signaling group to one SIP trunk group:

- Setting up the signaling groups
- Assigning members from more than one signaling group to one SIP trunk group

Related links

Assigning members from more than one signaling group to one SIP trunk group on page 1047
Setting up the signaling groups on page 1047

Screens for administering multiple signaling groups in one SIP trunk group

Screen name	Purpose	Fields
Signaling Group	Set up the signaling group.	• Group Type • IMS Enabled • Peer Detection Enabled • Peer Server
Trunk Group	Assign members from one or more signaling groups to one SIP trunk group.	• Member Assignment Method • Port • Sig Grp

Setting up the signaling groups

Procedure

1. Enter `add signaling-group n`, where *n* is the signaling group number.
2. Ensure that the **Group Type** field is set to SIP.
3. Set the **IMS Enabled** field to n.
4. Set the **Peer Detection Enabled** field to y.
5. Set the **Peer Server** field to Others.
6. Ensure that the **Q-SIP** and **Far-end Domain** fields have the same values for all signaling groups assigned to the SIP trunk group.
7. Set the **Enable Layer 3 Test** field to y.

   This ensures that Communication Manager maintenance detects a signaling group outage and enables trunk group member selection to bypass out-of-service signaling groups.
8. Select **Enter** to save your changes.

Assigning members from more than one signaling group to one SIP trunk group

Procedure

1. Enter `add trunk-group n`, where *n* is the trunk group number.
2. Ensure that the **Group Type** field is set to SIP.
3. Set the **Member Assignment Method** field to manual.

   The **Signaling Group** and **Number of Members** fields disappear.

4. On the Group Member Assignments page:
   a. Enter `IP` in the **Port** field.
   b. (Optional) Enter the SIP signaling group name in the **Name** field.
   c. Enter the SIP signaling group number in the **Sig Grp** field.

      You must assign different signaling groups in cyclical order for subsequent members of the trunk group. For example, if you have three signaling groups, such as 1, 2, and 3, assign the groups in the order 1, 2, 3, 1, 2, 3, 1, 2, 3, and so on for the subsequent members of the trunk group. This ensures that load balancing occurs amongst the different signaling groups.
5. Select **Enter** to save your changes.

Chapter 131: Music-on-Hold

Use the Music-on-Hold feature to automatically provide music, silence, or tone to a caller who:

- Is on hold
- Is transferred
- Is parked
- Waits in a queue

Detailed description of Music-on-Hold

Use the Music-on-Hold feature to automatically provide music, silence, or tone to a caller. The table on page 1049 shows the audio options that you can provide to a user.

Table 83: Music, silence, and tone options

Caller status	Music	Silence	Tone
On hold	Yes	No	Yes
On a trunk call that is being transferred	Yes	Yes	No
Parked	Yes	No	Yes
Waits in a queue	Yes	No	Yes

Note:

If you use equipment that rebroadcasts music or other copyrighted materials, you might be required to obtain a copyright license from, or pay fees to, a third party such as the American Society of Composers, Artists, and Producers (ASCAP), or Broadcast Music Incorporated (BMI).

Music-on-Hold administration

The following tasks are part of the administration process for the Music-on-Hold feature:

- Assigning music tones, music ports, and music for transferred trunks

- Defining a Class of Restriction for Music-on-Hold
- Connecting a music source to the server
- Assigning a source of music to a port

Related links

Assigning a source of music to a port on page 1052
Connecting a music source to the server on page 1052
Defining a Class of Restriction for Music-on-Hold on page 1051
Assigning music tones, music ports, and music for transferred trunks on page 1050

Screens for administering Music-on-Hold

Screen name	Purpose	Fields
Feature-Related System Parameters	Assign music tones, music ports, and music for transferred trunks.	• Music/Tone On Hold • Music Port • Music (or Silence) on Transferred Trunk Calls
Music Sources	Assign a music source to a port.	All
CPE Trunk Group	Connect a music source to the server.	All
Class of Restriction	Define a Class of Restriction (COR) for Music-on-Hold.	Hear System Music on Hold

Assigning music tones, music ports, and music for transferred trunks

Procedure

1. Enter `change system-parameters features`.
2. In the **Music/Tone on Hold** field, perform one of the following actions:
   - If you want a caller who is on hold to hear music, type `music`.
   - If you want a caller who is on hold to hear a tone, type `tone`.
   - If you want a caller who is on hold to hear neither music nor a tone, type `none`.

   If the **Tenant Partitioning** field on the Optional Features screen is set to y, you cannot administer the **Music/Tone on Hold** field. If the **Tenant Partitioning** field on the Optional Features screen set to y, you must use the Music Sources screen to assign music to a port.

   When you enter `music`, the system displays the **Type** field. Type one of the following values:

   - Type `ext` and the corresponding extension number of the music-on-hold.
   - Type `group` and the corresponding music-on-hold group number.

- Type `port` and the corresponding port location of the music-on-hold. The table on page 1051 shows how to construct a port number. You must specify a port on any supported analog line media module.

  For more information on music-on-hold groups see Locally Sourced Announcements and Music.

Table 84: Port field values

Characters	Description	Value
1-3	Gateway number	G4xx Media Gateway Number
4	Gateway	V
5	Slot number	1 through 8
6-7	Circuit number	Port number on media module
x	Administration without Hardware	If the **Secondary data module?** field, is set to n, you can type `x` in the **Port** field. A **Port** field set to x indicates that no hardware is associated with the port assignment.

3. In the **Music (or Silence) On Transferred Trunk Calls** field, perform one of the following actions:
   - If you want all transferred trunk calls to receive music until the call is answered, type `all`.
   - If you want a caller on the trunk call to hear music while the caller waits to be transferred, or ringback tone as soon as the transfer is complete, type `no`.

     The caller on the trunk call hears neither music nor a tone if Music-on-Hold is not administered.
   - If you want a trunk call that transfers to a station, and then waits at the station, to hear music, if music is administered, type `call-wait`.

     All other transferred trunk calls receive the ringback tone.
4. Select **Enter** to save your changes.

Defining a Class of Restriction for Music-on-Hold

Procedure

1. Enter `change cor n`, where *n* is the Class of Restriction (COR) to which you want to add Music-on-Hold.
2. In the **Hear System Music on Hold** field, perform one of the following actions:
   - If you want Music-on-Hold to be activate at a telephone, type `y`.
   - If you do not want Music-on-Hold to be activate at a telephone, type `n`.
3. Select **Enter** to save your changes.

Connecting a music source to the server

Procedure

Enter `add trunk-group next`.

You use the customer-premises equipment (CPE) trunks to connect a music source to the server.

For more information on how to administer trunk groups, see *Administering Avaya Aura® Communication Manager*.

Assigning a source of music to a port

Procedure

1. Enter `change music-sources`.
2. In the **Type** field, perform one of the following actions:
   - If you want the user to hear music, type `music`.
   - If you want the user to hear the tone-on-hold tone, type `tone`.

     You can specify tone for only one music source on the Music Sources screen.
   - If you want the user to hear neither music nor a tone, type `none`.
3. In the **Source** field, type the auxiliary trunk address, the analog port address, the group address, or the extension address of the music source.

   You cannot enter duplicate addresses in the **Source** field.

   The system displays the **Source** field only if you typed `music` in the **Type** field.

   The table on page 1051 shows you how to construct a port number.
4. In the **Description** field, type a maximum of 20 characters that describe the source of the music.

   The system displays the **Description** field, only if you typed `music` or `tone` in the **Type** field.
5. Select **Enter** to save your changes.

Considerations for Music-on-Hold

This section provides information about how the Music-on-Hold feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Music-on-Hold under all conditions. The following considerations apply to Music-on-Hold:

- If the **Tenant Partitioning** field on the Optional Features screen is set to y, you cannot administer the **Music/Tone on Hold** field on the Feature-Related System Parameters screen. If the **Tenant Partitioning** field on the Optional Features screen set to y you must use the Music Sources screen to assign music to a port.

- Any number of calls can simultaneously connect to music.
- The system does not provide music to callers, in a multicaller connection, who are in a queue, on hold, or parked.

Note:

The system wide analog port configured for Music-on-Hold or the analog port configured as the first entry on Music Sources form, are not accounted for Port Sensitive Pricing.

Interactions for Music-on-Hold

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

Automatic Call Distribution (ACD)

If you administer Music-on-Hold to provide music, the system provides the music after the ACD split delayed announcement.

Data Privacy and Data Restriction

If a user or an attendant places a call that has either Data Privacy or Data Restriction activated on hold, the system withholds Music-on-Hold. The system withholds Music-on-Hold to prevent transmission of a musical tone that a connected data service might falsely interpret as a data transmission.

Hunting

If you administer Music-on-Hold to provide music, the system provides the music after the Direct Departmental Calling (DDC) group or the uniform call distribution (UCD) group delayed announcement.

If Music-on-Hold is not administered, then there will be no ring-back (a silence will be played) after delayed announcement is played (administered for non ACD hunt) and till an agent gets available. To avoid this silence, either Music-on-Hold should be administered or delayed announcement should be of type "integ-mus".

Note:

When you deactivate the 7.0.1 patch, the system runs on 7.0 system and sets the **Live Stream Source** feature to **n**. Therefore, you must install and activate the new 7.0.1 patch immediately to prevent the system processes from running on the 7.0 system. You must also set the value of the **Live Stream Source** feature to **y**.

Chapter 132: Names Registration

Names Registration automatically sends a guest's name and room extension from the PMS to Communication Manager at check-in, and automatically removes this information at checkout.

Detailed description of Names Registration

The information provided by Names Registration displays on any attendant console or display-equipped phone (as might be used for example, by Room Service, Security, and others). Hotel personnel can use the information provided by the names Registration screen to greet their calling guests with personalized greetings. For example, if John Smith calls room service, personnel with a display-equipped phone, see John's name and room extension and can answer with a personalized greeting.

The name of the calling or called party can display on display-equipped phones. To maintain necessary guest security, hotels do not divulge guests' room numbers to other guests or callers. For this reason, do not assign display-equipped phones to guest rooms.

Checking in

Procedure

1. Information about the guest is obtained and stored in the hotel's PMS.
2. The PMS sends a check-in message to Communication Manager.
3. Communication Manager stores the guest's name and coverage path.
4. Communication Manager removes the outward restriction on the telephone in the guest room. Communication Manager removes all LWC messages.
5. Communication Manager changes the status of the room from unoccupied to occupied.

   At check-in, update the PBX names internal table and the call-coverage path for the guest phone. Names Registration automatically sends a guest's name, extension (room), and preferred call-coverage path to Communication Manager.

Checking out

Procedure

1. Communication Manager clears any previous wakeup calls.

2. Communication Manager clears message-waiting lamp indications.
3. Communication Manager activates controlled outward restriction, removes the guest's name, and identifies any unopened messages.

   At checkout, Names Registration automatically changes the call-coverage path to the administered Default Coverage Path for Client Rooms.

Guest Information Input/Change

Use Guest Information Input/Change to change the guest name associated with an extension, input a guest name after check-in, or change a call-coverage path. For example, hotel may check in airline personnel before their arrival to guarantee their reservation. However, hotel personnel may be unaware of the guests' names and so wait until their arrival to update the names.

Names Registration Information Format

For both Names Registration and Guest Information Input/Change, a guest name may consist of as many as 15 characters, including spaces and commas. Do not use periods.

The name may be in all upper case letters, all lower case letters, or a mixture of upper case and lower case letters. To use Integrated Directory, enter the name using one of the following methods.

- Last name, comma, first name (for example, Jones, Fred)
- Last name, comma, first name, space, title/middle initial/name (for example, Jones, Fred Mr)
- Last name only (for example, Jones)

Call Coverage for Names Registration

Both Names Registration and Guest Information Input/Change messages contain call-coverage path numbers. These numbers do not display but are used to configure the appropriate call-coverage arrangements for guest extensions. Arrangements can be for voice mail, text messages, any available coverage point, or no coverage at all.

Administer call-coverage paths on Communication Manager, and use the associated path numbers to establish coverage arrangements at check-in. For suites, administer paths to allow one room in the suite to be the coverage point for the other. To make customized arrangements at time of check-in (such as coverage from one guest room to another), manually administer the path attributes at Communication Manager.

Considerations for Names Registration

This section provides information about how the Names Registration feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Names Registration under all conditions. The following considerations apply to Names Registration:

- Call-coverage path numbers sent by PMS to Communication Manager for automatic reconfiguration are limited to those administered on Communication Manager and stored in PMS.
- A guest room extension can have a maximum of 5 digits.
- An input in PMS of the name displayed on display-equipped phones updates Communication Manager.
- The **Name and Room Number/Extension** is not overwritten with a redirection reason unless the call is an emergency call or the station always is administered to have redirection. Also, certain redirection displays will not be shown (for example, priority, intercom dialing).

Interactions for Names Registration

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

Call Coverage

Call-coverage arrangements are not limited to automatic update during check-in messages sent from PMS. Hotel personnel require coverage points other than those designated for guests. Call-coverage paths can be manually administered at the server via the system management terminal.

COS

If an extension has a client room COS, the save translation operation clears the station name and sets the coverage path to the default coverage path for client room when stored on tape. This does not affect the existing information in memory. However, if the translations are read in, it affects existing extensions until a database swap synchronizes Communication Manager and PMS.

Name Character Length

Communication Manager supports 27-character names, but the PMS interface supports only 15-character names.

PMS Interface

During a Room Change/Room Swap, the name originally associated with the first terminal is changed or swapped to the second terminal along with call-coverage path, automatic wake-up entries, message-waiting status, and controlled restrictions.

Chapter 133: Night Service

Use the Night Service feature to direct incoming calls to other answering points at night.

Detailed description of Night Service

Communication Manager provides the following Night Service capabilities:

- Hunt Group Night Service
- Night Console Service
- Night Station Service
- Trunk Answer from Any Station
- Trunk Group Night Service

Hunt Group Night Service

With Hunt Group Night Service, an attendant or a split supervisor can assign a hunt group or a split to Night Service mode. All calls for the hunt group then are redirected to the hunt group's designated Night Service Extension (NSE). When a user activates Hunt Group Night Service, the associated button lamp lights.

Night Console Service

Night Console Service directs all calls for primary and daytime attendant consoles to a night console. When a user activates Night Console Service, the Night Service button for each attendant lights, and all attendant-seeking calls (and calls that are waiting) in the queue, are directed to the night console.

To activate and deactivate this feature, the attendant usually presses the **Night** button on the principal attendant console or a designated console.

Night Station Service

Night Station Service directs incoming calls for the attendant to designated extensions. To activate Night Station Service, attendants press the **Night** button on the principle console, if there is an inactive night console. If the night station is busy, calls including emergency attendant calls, receive busy tone. Calls do not queue for the attendant.

When Night Station Service is active, the system routes the incoming calls to the attendant as follows:

- Direct Inward Dialing (DID) Listed Directory Number (LDN) calls are routed to a designated DID-LDN night extension.
- Internal calls route to the DID -LDN night extension, unless you administer the system so only DID-LDN calls can route to the LDN night extension.
- Non-DID calls are routed to the night destination that you specify for the trunk group or for the individual trunk. If you do not specify a night destination, the calls route to the DID-LDN night extension.

You can assign a unique extension as the night destination for each incoming central-office, foreign-exchange, or 800-Service trunk group. Both the extension assigned as a trunk group's night destination and the DID-LDN night extension can be phones or answering groups (such as DDC group, UCD group, or terminating extension group (TEG).

TAAS with Night Service

With Trunk Answer from Any Station (TAAS), telephone users can answer all incoming calls to the attendant when the attendant is not on duty, and when other telephones are not designated to answer the calls. The incoming call activates a gong, a bell, or a chime and a telephone user dials an access code to answer the call.

Users can activate TAAS if each of the following conditions is met:

- The attendant pressed the **Night** button on the primary console or a user (if Communication Manager has no attendant administered) pressed the **Night Service** button on the designated Night Service phone.
- A night console is not assigned or is not operational.
- Night Station Service is inactive.

Trunk Group Night Service

With Trunk Group Night Service, an attendant or a designated Night Service telephone user can assign one or all trunk groups to Night Service mode. When a user activates Night Service, trunk groups that are assigned a Trunk Group Night Service termination change to Individual Trunk Night Service mode. The system redirects the calls that come into the trunk group to the group's designated NSE. Incoming calls on trunk groups that are not assigned to Trunk Group Night Service are queued in the attendant queue. If the call remains unanswered during the Night Service Disconnect Timer interval, the incoming trunk disconnects.

A user can also assign all the trunk groups to the Night Service mode at the same time. Then all the trunk groups are in the System Night Service mode. The system redirects any incoming calls made on the trunk groups to their designated NSE for the trunk group. To assign all the trunk groups to System Night Service, the user presses the **System Night Service** button on the principal attendant console or the **Night Service** button on a designated phone. You can assign a Night Service button to only one telephone.

To activate Trunk Group Night Service, you press the individual Trunk Night Service buttons on the attendant console or on a telephone. You can assign Trunk Night Service buttons on more than one telephone.

Night Service administration

The following tasks are part of the administration process for the Night Service feature:

- Setting up night station service to voice mail
- Setting up Night Console Service
- Setting up Night Station Service
- Setting up TAAS for Night Service
- Setting up TAAS external alerting
- External alerting Night Service set up
- Setting up Night Service for trunk groups
- Setting up Night Service for hunt groups

Related links

Setting up Night Service for hunt groups on page 1063
Setting up Night Service for trunk groups on page 1062
External alerting Night Service set up on page 1062
Setting up TAAS external alerting on page 1062
Setting up TAAS for Night Service on page 1061
Setting up Night Station Service on page 1061
Setting up Night Console Service on page 1061
Setting up night station service to voice mail on page 1060

Screens for administering Night Service

Screen name	Purpose	Fields
Hunt Group	Set Night Station Service to voice mail.	Group Number
Listed Directory Number		Night Destination
Console Parameters		DID-LDN Only to LDN Night Ext
Attendant Console	Set up Night Console Service.	Console Type
Listed Directory Numbers	Set up Night Station Service.	Night Destination
Console Parameters		DID-LDN Only to LDN Night Ext
Feature Access Codes	Set up Trunk Answer from Any Station (TAAS)	Trunk Answer Any Station Access Code

Table continues…

Screen name	Purpose	Fields
Console Parameters	Set up external alerting.	EXT Alert Port (TAAS)
Listed Directory Numbers	Set up external alerting night service.	Night Destination
Console Parameters		• EXT Alert Port (TAAS) • DID-LDN to Night Ext.
Trunk Group	Set up Trunk Group Night Service.	Night Service
Hunt Group	Set up Night Service for hunt groups.	Night Service Destination

Setting up night station service to voice mail

Procedure

1. Enter `add hunt-group next`.

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

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

   There can be no members in this hunt group.

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

   Note:

   If you are using tenant partitioning, the command for the next step is **`change tenant`** *n*. If you are using tenant partitioning, the Listed Directory Numbers screen does not display the **Night Destination** field. Instead, the **Night Destination** field is on the Tenant screen.

4. Enter `change listed-directory-numbers`.

5. In the **Night Destination** field, add the night destination for the listed directory phone number.

6. Select **Enter** to save your changes.

7. Enter `change console-parameters`.

8. In the **DID-LDN Only to LDN Night Ext** field, type `n`.

9. Select **Enter** to save your changes.

10. From a phone with console permissions, dial the call forwarding Feature Access Code, then the hunt group's extension, followed by the main number of Communication Manager Messaging.

    Note:

    You should receive a confirmation tone that consists of three beeps, which is default. This step is very important because calls to the LDN night service extension do not follow coverage.

11. In your voice mail, build the automated attendant with the extension of the Listed Directory Number (LDN), not the hunt group.

    The originally dialed number was the LDN, which is the number Communication Manager passes to the voice mail application. In the case of the Communication Manager Messaging voice mail systems, you can use the Auto Attendant routing table to send the calls to a common automated attendant mailbox.

Setting up Night Console Service

Procedure

1. Enter `change attendant n`, where *n* is the number of the attendant console.
2. In the **Console Type** field, type `principal`.

   The system can include only one night-only or one day/night console, unless you administer Tenant Partitioning. Night Service is activated from the principal console, or from the one station set per system that has a **nite-serv** button.
3. Select **Enter** to save your changes.

Setting up Night Station Service

Procedure

1. Enter `change listed-directory-numbers`.
2. Type the extension number in the **Night Destination** field.

   The destination can be an extension, a recorded announcement extension, a vector directory number, or a hunt group extension.
3. Select **Enter** to save your changes.
4. Enter `change console-parameters`.
5. In the **DID-LDN Only to LDN Night Extension** field, type `n`.
6. Select **Enter** to save your changes.

   After you set up night station service, you must have the attendant use the night console button to activate and deactivate night service.

Setting up TAAS for Night Service

Procedure

1. Enter `change feature-access-codes`.
2. Click **Next** until you see the **Trunk Answer Any Station Access Code** field.
3. In the **Trunk Answer Any Station Access Code** field, type the access code.

   In this example, the access code is 71.
4. Select **Enter** to save your changes.

Setting up TAAS external alerting

About this task

Once you set the FAC, you must determine where the external alerting device is connected to the server that is running Communication Manager.

Procedure

1. Enter `change console-parameters`.
2. In the **EXT Alert Port (TAAS)** field, type the port address that is assigned to the external alerting device.
3. Select **Enter** to save your changes.

External alerting Night Service set up

Sending LDN calls to the security guard at night

Procedure

1. Enter `change listed-directory-numbers`.
2. In the **Night Destination** field, verify that this field is blank.
3. Select **Enter** to save your changes.
4. Enter `change console-parameters`.
5. In the **EXT Alert Port (TAAS)** field, type the port address that is assigned to the external alerting device.
6. Select **Enter** to save your changes.

Sending LDN calls to the TAAS bell at night

Procedure

1. Enter `change console-parameters`.
2. In the **DID-LDN Only to Night Ext.** field, type `y`.

   With this setting, only LDN calls can go to the Listed Directory Night Service Number Extension.
3. In the **Ext Alert Port (TAAS)** field, type the port address that is assigned to the external alerting device.
4. Select **Enter** to save your changes.

Setting up Night Service for trunk groups

Procedure

1. Enter `change trunk-group` *n*, where *n* is the number of a trunk group.
2. In the **Night Service** field, type the extension number that you want the calls to go to.

The destination can be a station extension, a recorded announcement extension, a vector directory number (VDN), a hunt group extension, a terminating extension group (TEG), or attd if you want to direct the call to the attendant.

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

Setting up Night Service for hunt groups

Procedure

1. Enter `change hunt-group n`, where *n* is the number of a hunt group.
2. In the **Night Service Destination** field, type the extension number.

   The destination can be an extension, a recorded announcement extension, a VDN, a hunt group extension, attd if you want to direct calls to the attendant.
3. Select **Enter** to save your changes.

Considerations for Night Service

This section provides information about how the Night Service feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Night Service under all conditions.

Considerations for Hunt Group Night Service

- Both Hunt Group Night Service and Trunk Group Night Service can be active at the same time. An incoming trunk call is redirected to the trunk group's designated NSE. If this NSE is a hunt group or split that is in Hunt Group Night Service mode, the call is redirected to the Hunt Group NSE.
- Calls in progress (such as talking, on hold, or waiting in queue) on the hunt group or split are not affected when the hunt group or split is set on the Hunt Group Night Service mode.
- When a hunt-group queue becomes empty, all idle members are placed in a busy condition.
- If Night Service is activated for a hunt group or split and a power failure occurs, the hunt group or split automatically returns to the Night Service mode.

Considerations for Night Console Service

- The night console must be identical to and have the same features as the primary console. A daytime console can double as the night console.
- Night Console Service calls to the attendant group are still handled by an attendant, even though the primary and daytime attendant consoles are out of service.
- The system supports only one night console. The night console can be activated only when the primary and daytime consoles have been deactivated.

- If Night Console Service is active and a power failure occurs, the system automatically returns to Night Console Service mode when it is powered up.

Considerations for Night Station Service

- When Night Station Service is active but you have not established Night Station extensions, a user can activate TAAS.
- You can assign a Night-Serv button to either an attendant extension or a phone extension. An individual trunk group or hunt group can be put into night service by either an attendant extension or a phone extension with the necessary button. When a user presses this button to activate Night Station Service, all calls to that particular trunk group or hunt group are routed to the Night Service extension assigned to that group.
- If a trunk without disconnect supervision goes to Night Service, the system drops the trunk after a period of time to avoid locking up the trunk. The call is not routed to the DID-LDN night extension.

Considerations for TAAS

- If Night Service is active and a power failure occurs, the system, when brought back up, automatically returns to Night Service mode.

Considerations for Trunk Group Night Service

- All incoming calls on Night Service trunk groups go to the trunk group's NSE unless the trunk group member has its own Trunk Group Member Night Destination, in which case the calls are redirected to that destination instead of the trunk group's NSE.
- Calls already in progress on a trunk group (such as talking, on hold, or waiting in queue), are unaffected when the individual Trunk Group Night Service or System Night Service is activated.
- Trunk Group Night Service and System Night Service work independently of one another.
  - When a user activates System Night Service, any trunks that are controlled by individual Trunk Group Night Service buttons remain in day service. Trunk groups that are not currently assigned to Trunk Group Night Service are assigned to System Night Service.
  - Trunks with individual Trunk Group Night Service can be removed from Night Service even though the rest of the system remains in Night Service.
  - When a user deactivates System Night Service, any trunks that have individual Trunk Group Night Service still active remain in night service.
  - Trunks with individual Trunk Group Night Service can be placed into Night Service even though the rest of the system remains in day service.
- If a trunk is added to a trunk group while that trunk group is in Trunk Group Night Service, the trunk is brought up in night service.
- Individual Trunk Group Night Service does not apply to DID trunk groups.

- If Night Service is activated for a trunk group, and a power failure occurs, the trunk group automatically returns to the Night Service mode.
- If for some reason, a phone with a trunk-ns button remains out of service after a system reboot and later comes back in service, the trunk-ns lamp shows the trunk status within 10 seconds of coming back in service. For example, a telephone with a trunk-ns button might be unplugged when the system is rebooted. If the phone is plugged back in later, the trunk status is shown on the trunk-ns button within 10 seconds.

Interactions for Night Service

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

Interactions for Hunt Group Night Service

Automatic Call Distribution (ACD)

When Hunt Group Night Service is active for a split and the night-service destination is a hunt group, the caller hears the first forced announcement for the original split. The system then redirects the call to the Night Service destination hunt group. When an agent in the Night Service hunt group becomes available, the call goes to that agent. If all agents in the hunt group are busy, the caller hears the following: forced or delayed first announcement, ringback, music-on-hold or silence, and a second announcement.

Call Coverage

Coverage takes precedence over Night Service. When Hunt Group Night Service is active, the NSE’s normal coverage criteria and path apply. If the coverage path destination is Communication Manager Messaging, Communication Manager Messaging answers with the mail of the original hunt group. If the NSE is a hunt group or split of any type, the hunt group or split’s call coverage criteria and coverage path apply. The coverage criteria and path can be different from that assigned to the phones that are members of that hunt group or split.

If a coverage point is a hunt group or split in Night Service, the system considers the point to be unavailable and does not forward the call to the coverage point’s NSE.

Call Forwarding All Calls

If a hunt group or split is in Hunt Group Night Service mode and the hunt group or split’s NSE has Call Forwarding - All Calls active, the system forwards night-service calls terminating to that NSE to its designated call-forward extension.

If the forwarded-to destination is a hunt group or split in Night Service mode, the system terminates the call at the forwarding extension.

Interactions for Night Console Service

Trunk Group Night Service

Activation of Night Console Service for the attendant consoles also puts trunk groups into night service, except those trunk groups for which you administered a Trunk Group Night Service button.

Interactions for Night Station Service

Call Coverage

Calls routed to the night extension using Night Station Service follow the coverage path of the night extension under all coverage criteria except Send All Calls.

If a night extension has a coverage path in which Cover All Calls is administered, all attendant-seeking calls redirect to coverage. Changes to the protocol for handling DID-LDN calls (that is, forwarding attendant-seeking calls on or off premise from the night extension) do not work.

Call Forwarding All Calls

Calls redirected to the attendant through Call Forwarding All Calls do not route to the DID-LDN extension.

Inward Restriction

Inward-restricted phones can be administered for Night Station Service. Night Service features override Inward Restriction.

Night Console Service

Do not provide Night Console Service with this Night Station Service.

Remote Access

A Remote Access extension can be specified as the Night Station extension on an incoming, non-DID, trunk group.

Tenant Partitioning

Each tenant may have a designated night-service station. The system directs calls to an attendant group in night service to the night-service station of the appropriate tenant (when a night attendant is unavailable). When someone places an attendant group into night service, all trunk groups and hunt groups that belong to tenants served by that attendant group go into night service. In this case, the system routes incoming calls to the night-service destination of the appropriate tenant.

Each tenant can have its own LDN night destination, TAAS port, or night attendant.

Timed Reminder

Timed Reminder calls returning to a console that has been placed in Night Service and has an assigned DID-LDN night extension is not redirected to the DID-LDN night extension. Rather, they are dropped.

Trunk Answer from Any Station

TAAS and Night Station Service can both be assigned within the same system, but cannot be assigned to the same trunk group.

Interactions for TAAS

Call Coverage

If Night Station Service is active, calls that are redirected to the attendant through Call Coverage can be answered by way of TAAS.

Call Forwarding All Calls

If Night Station Service is active, calls that are redirected to the attendant through Call Forwarding All Calls can be answered by way of TAAS.

Inward Restriction

Inward-restricted phones can activate TAAS for incoming trunk calls. Night Service features override Inward Restriction.

Night Console Service

Do not provide a Night Console Service with TAAS.

Night Station Service

TAAS and Night Station Service can both be assigned within the same system, but cannot be assigned to the same trunk group. Activating Night Station Service also activates Night Service - Trunk Group for any trunk group without an individual trunk-group Night Service button.

Tenant Partitioning

Each tenant can have its own LDN night destination, TAAS port, or night attendant.

Interactions for Trunk Group Night Service

Call Forwarding All Calls

If the individual Trunk Group Night Service mode and the trunk group's NSE have Call Forwarding All Calls activated, the night service calls that terminate to that NSE are forwarded to the designated extension.

Forced First Announcements

An interaction occurs with System Night Service and Forced First Announcement. For example, if hunt group A has a forced first announcement, assign the incoming CO trunk to terminate at hunt group A. Assign the incoming trunk's night-service destination to be another hunt group (hunt group B). Assign a Night Service button to the attendant.

With night service active on the attendant, the incoming CO call routes to the night-service destination hunt group B and does not play the Forced First Announcement of the incoming destination's hunt group A.

Listed Directory Number

In System Night Service mode, all incoming LDN calls (except those using DID trunks) which have activated night service are redirected to their corresponding trunk group's NSE. Incoming LDN calls using DID trunks are directed to the Night Console Service, Night Station Service, or Trunk Answer From Any Station, respectively, whichever applies first. Non-LDN DID trunk calls terminate at the dialed extension.

Vector Directory Number

If a system is in night service mode and you have assigned a VDN number in the **Night Serv** field of the Incoming Call handling treatment form, the system routes the inbound call to all the configured VDNs and then to an agent. The telephone display of the agent shows the name of the first VDN, which you assigned in the **Night Serv** field.

Chapter 134: 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.

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

This feature provides two classifier modes:

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

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

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

Note:

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

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

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

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

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

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

Call processing scenarios

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

ISDN trunk

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

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

SIP trunk

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

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

- Communication Manager has received an answer signal from the far end of the trunk.

Other trunks (Non-ISDN & Non-SIP)

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

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

Mixture of old and new classifiers

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

End OCM timer

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

Active VDN

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

Administering No-cadence call classification modes and End OCM timer

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

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

This section describes:

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

Related links

Setting up no-cadence call classification modes on page 1072
Setting up End OCM timer and announcement extension on page 1072

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

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

Setting up no-cadence call classification modes

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.

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

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

Announcements

To prevent delays while connecting the announcement,

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

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

Performance impact

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

Call Management System (CMS) and Avaya IQ

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

AMD false positives

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

Ringing regulation

A call center can allow outbound calls to ring for certain amount of seconds if the calls are not answered by the call receiving party. The ringing regulation varies from country to country. To satisfy the regulation of your land, you must do the following:

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

Tenant

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

the End of OCM Intercept Extension field with a single VDN which in turn routes the call to the correct announcement for each tenant.

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

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

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

Multi-National/Global Considerations

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

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

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

TTY classification

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

Call classification after answer supervision

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

CONNECT reliable when call leaves ISDN

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

Answer supervision timeout

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

Private network ISDN (QSIG)

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

- The outgoing trunk uses private network QSIG signaling.

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

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

SIP

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

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

CCRON

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

EC500

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

Call vectoring

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

Inter-Gateway Alternate Routing

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

Call Redirection

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

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

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

Uniform Dial Plan

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

Multi-location ARS routing

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

- Communication Manager terminates an OCM call to the End of OCM Intercept Extension.

- **End of OCM Intercept Extension** is administered as a VDN.
- Associated vector has a route-to step.

Multi-Location Dial Plan (MLDP)

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

Chapter 135: Off-Premises Station

Use the Off-Premises Station feature to connect a telephone that is in a different building than the server that runs Communication Manager to your system.

Detailed description of Off-Premises Station

With the Off-Premises Station feature, you can connect a telephone that is located in a different building than the server that runs Communication Manager to your system.

If you use central office (CO) trunk circuits, the telephone must be:

- Analog
- FCC registered, if the telephone is in the United States
- Registered by the appropriate governmental agency, if the telephone is located outside the United States

You can use digital communications protocol (DCP) sets as off-premises telephones if you add IP Softphone or IP Office. You can set up IP stations as off-premise stations if you use point-to-point protocol (PPP) connections. DS1 trunk service provides a digital interface for off-premises stations.

A trunk-data module connects off-premises private-line trunk facilities and Communication Manager. The trunk-data module converts between the RS-232C and the DCP, and can connect to Direct Distance Dialing (DDD) modems as the DCP member of a modem pool.

Off-Premises Station requires cross-connecting capabilities, and one port on an analog line or a DS1 tie trunk media module for each interface that you want to provide. Not all analog lines can support an off-premises station. For more information, see the user guide for the appropriate telephone.

The maximum loop distance for off-premises stations is 20,000 feet (6093.34 meters) if you do not use repeaters. For information about the cable distance, see the user guide for the appropriate telephone.

Note that the system does not support the use of a message waiting indicator lamp (MWI) on an off-premises station.

Off-Premises Station administration

The following task is part of the administration process for the Off-Premises Station feature:

- Activating Off-Premises Station for a user

Related links

Activating Off-Premises Station for a user on page 1078

Screens for administering Off-Premises Station

Screen name	Purpose	Fields
Station (analog)	Activate an off-premises station for a user.	• Off Premise Station • Balance Network

Activating Off-Premises Station for a user

Procedure

1. Enter `change station n`, where *n* is the extension of the user for whom you want to activate an off-premises station.
2. In the **Off-Premises Station** field, perform the following actions:
   - If the telephone associated with this Station screen is not located in the same building as the server, type `y`.

     If you type `y`, you must administer the **R Balance Network** field on the Station screen.
   - If the telephone associated with this Station screen is located in the same building as the server, type `n`.
3. In the **R Balance Network** field, perform one of the following actions.
   - Type `y` to select the R Balance Capacitor network. Type `y` in all other cases, except for the following cases:
   - Type `n`:
     - To select the standard resistor capacitor network
     - When the station port circuit is connected to the terminal equipment. Terminal equipment includes, for example, SLC carriers or impedance compensators. These are optioned for 600-ohm input impedance and the distance between the server and the equipment is less than 3,000 feet (914.4 meters).

   You must complete the **R Balance Network** field if the **Off-Premises Station** field on the Station screen is set to y.

Interactions for Off-Premises Station

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

Distinctive Ringing

The Distinctive Ringing feature might function improperly at an off-premises telephone because of the distance of the telephone from the server. However, the Distinctive Ringing feature can be disabled when you set the **Off-Premises Station** field on the Station screen to y. If the Distinctive Ringing feature is not used with an off-premises station, the telephone receives one-burst ringing for all calls.

Chapter 136: Offline call journal

Online/Offline Call Journal (Call History) for H.323 endpoints

Previously, the H.323 phones were responsible for maintaining the call logs. As long as the users were logged in to the phone, the phone backed up all call logs. After the user logged out and logged back in, the phone pulled the previously stored call logs. However, these logs did not contain incoming calls that took place while the user was logged out. This behavior led to confusion as all the registered devices did not show the same call logs if the user was logged in to some devices and not others.

From Communication Manager Release 6.3.6, call logs include the incoming calls even when the device is in the logged-out state. This support is available to the latest H.323 endpoints. Communication Manager stores up to 10 entries for the most recent calls for the user. When the user logs back in, Communication Manager sends these log entries to the phone. The H.323 phone reconciles the call logs it receives from Communication Manager with the logs it restores from the backup server. The H.323 phone backs up the merged call logs in the central backup file for later retrieval. The H.323 phones back up the call logs to an HTTP server and load whenever a user logs in.

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

Detailed description for Offline Call Journal

Earlier, H.323 phones used HTTP to back up and restore the call logs to the Apache server. But, any calls received while the phone is logged out were not reported to the user upon login. SIP desk phones stored the call logs in the phone because the SIP desk phones did not have any central storage. When a SIP user logged in from a different desk phone, the user could neither see the old call log history nor any information about the calls received while the phone was logged out.

With this enhancement, the H.323 and SIP desk phones back up all the call logs and restore them when the user logs in. Communication Manager backs up up to 10 calls for the logged-out H.323 users. The H.323 station stores the call logs when the user has logged into the station. Session Manager backs up up to 100 calls per station for the logged in and logged-out SIP users.

Offline Call Logging

Use the **Offline Call Logging** field to back up and restore call logs for an offline user.

Valid entry	Usage
y	Communication Manager tracks the calls that the user missed when the telephone was in the logged-out state, and updates the call logs on the telephone when the user logs in. The default option is y.
n	Communication Manager does not track the calls that the user missed when the telephone was in the logged-out state.

Administering Offline Call Journal for H.323 stations

About this task

Use this procedure to administer Online Offline Call Journal feature for H.323 stations.

Procedure

1. Type change station *n*, where *n* is the name of the station.
2. Press `Enter`.

   The system displays the Station screen.
3. On page 3, ensure that the **Offline Call Logging** field is set to `y`.
4. Save the changes.

Administering Offline Call Journal for SIP stations

About this task

Use this procedure to enable Offline Call Journal for SIP stations.

Procedure

1. In System Manager, go to **User Management** > **Communication Profile** .
2. Enable **Call History**.
3. Save the settings.

Example

Interactions for Offline Call Journal

Call Pickup Alerting Group

If a member of a call pickup group receives a call when the extension is logged out, the member does not receive any incoming call alert. If the call is missed, other members of the group do not receive any missed call notification. If you enable the History flag for the extension, the missed calls get logged in the call history of the extension. When the user logs back in to the extension, the telephone displays a missed call on the top line and the History LED is lit.

The member can add the contact from the missed call history to the contacts list. The member can also track the presence state of the contact from the missed call history screen. For example, if the telephone of the contact whose call is missed is locked, the presence state of that contact appears as *Away* on the History screen of the member who missed the call.

Autocall back feature

If the autocall back feature is active on the extension of the caller, the caller receives a call back from Communication Manager as soon as the called party becomes available. If the caller is logged out, the caller receives a busy tone.

After the caller logs back in to the extension, the telephone displays a missed call on the top line and the History LED is lit.

Clearing All History Log

Users can clear the missed call logs from the History screen.

Send All Calls

If a user activates the Send All Call (SAC) feature and sets the coverage path to voicemail, the telephone records the missed calls in the call history. When the user logs back in, the user sees the missed call notification on the History screen.

If SAC is active on the station, do not select the Cover All Calls (CAC) redirection criteria. Both the redirection features redirect incoming calls to the coverage path. However, redirection in SAC takes place by a button push or by dialing a FAC. If you enable SAC with the Cover All Calls criterion, the station stores duplicate entries in the call history log.

Changing language

A user can change the language of the call log history by changing the language of the phone.

Call park and unpark

A call that is put on hold on one extension and retrieved from another gets recorded in the call history log of the phone from where the call is retrieved.

EC500

Endpoints with EC500 support the offline call journaling feature. For example, if A activates EC500 on the phone and logs out of the extension, any missed call gets recorded in the call history log of the phone of A.

Bridged Call Appearance

If a phone has a bridged call appearance of another phone, any call missed by the primary number, whose extension is bridged on to, is recorded in the call history log of the phone that has the bridged call appearance.

For example, A has the bridged call appearance of B. When A logs out of the extension and B misses a call, A can view the missed call in the call history log after A logs in to the extension.

CPN blocking

The CPN blocking feature is supported with the offline call log feature. If a user activates the CPN blocking feature on the extension, missed calls are recorded in the call history log. When the user logs back in to the extension, the user sees two missed call notifications and the lit History LED. The call history log shows the contact name of the missed entry as *anonymous.*

Call Forward feature

If the call forwarding feature is active on an extension, any incoming call that is missed gets recorded in the call history log of the extension. The caller receives an error tone if the extension is logged out. After the user logs back in, the user sees the missed call notification and the lit History LED.

Multi-device access

If members of a multidevice access group are in the logged-out state, incoming missed calls are stored in the missed call history log of the devices. The caller receives an error tone because all the devices are logged out.

Shared control mode

If a deskphone is in the shared control mode, a missed call is logged in the call history log of the phone. For example, a user might have a deskphone and Avaya one-X® Communicator in the shared control mode. In this case, if both the devices are logged out, the missed calls are recorded in the call history of the devices.

Session Border Controller

A configuration consisting of Session Border Controller (SBC) also supports the Offline call journaling feature. For example, if a user outside an enterprise network receives calls from an enterprise network while the user is logged out, the telephone of the user stores the missed calls.

After the user logs in to the telephone, the user finds the missed call entries on the top line of the phone.

Failover and failback to primary Session Manager

If the primary controller fails, the phones registered to the primary controller move to the secondary controller. If a logged-out extension receives a call during this period, the call is not recorded in the call history log of the logged out extension. However, when the primary controller becomes active and the phones re-register to the server, the missed calls get recorded in the call history log of the logged out extension.

Failover to Branch Session Manager and failback to primary Session Manager

If the primary controller fails, the phones registered to the primary controller move to the secondary controller. If a logged-out extension receives a call during this period, the call is not recorded in the call history log of the logged-out extension. However, when the primary controller

becomes active and the phones re-register to the server, the missed calls get recorded in the call history log of the logged-out extension.

Failover to Branch Session Manager and failback to IP Office

If the primary controller fails, the phones registered to the primary controller move to the secondary controller. If a logged-out extension receives a call during this period, the calls are not recorded in the call history log of the logged-out extension. However, when the primary controller becomes active and the phones re-register to the server, missed calls get recorded in the call history log of the logged-out extension.

Chapter 137: Out of Band management

Out of Band Management

With the Out of Band Management feature, you can set up a dedicated network connection to securely manage Communication Manager. The network connection can be physical or virtual.

Detailed description of Out of Band Management

Communication Manager has a virtual NIC for a dedicated Ethernet connection for management functions. You can use System Management Interface (SMI) to manage the Avaya products using this dedicated Ethernet connection. The dedicated network connection administration persists after a Communication Manager upgrade.

With the dedicated network connection, you can create separate channels for the user functions and the management functions. You can use the dedicated network connection for the management functions to manage the system, perform IA scans, and update the firmware. You can also use the network connection for other network services such as system logging, backup, NTP, and WebLM licensing. For the user functions, you can set up more specific user access controls. You can also have more specific auditing processes to detect insider threats.

Out of Band Management administration

To configure the Out of Band Management of management data on Communication Manager, you must do the following:

- Depending on your Communication Manager configuration, assign an IP address and a subnetwork mask to the eth1 or eth2 Ethernet connection.
- Select Out of Band Management as the functional assignment.
- Enable Out of Band Management of management data.
- Add a static route between the Out of Band Management interface and the enterprise network.

Screens for administering Out-of-Band management

Screen name	Purpose	Fields
Network Configuration	Configure the IP address and the subnetwork mask to administer the Ethernet connection.	• **IPv4 Address** • **Mask** • **Functional Assignment** • **Restrict Management traffic to Out-of-Band interface is currently**
Status Routes	Create a static route between the Out-of-Band management interface and the enterprise network to route all management function data through the Out-of-Band management interface.	• **IP Address** • **Mask / Prefix** • **Gateway** • **Interface**

Administering the Out of Band Management of management data

Procedure

1. Log in to Communication Manager SMI.
2. Click **Administration** > **Server (Maintenance)**.
3. In the navigation pane, click **Server Configuration** > **Network Configuration**.
4. Configure the following **eth1** fields:
   - **IPv4 Address**: The IP address of the Ethernet connection
   - **Mask**: The subnetwork mask of the IP address
   - **Functional Assignment**: **Out-of-Band Management**

   If the Communication Manager instance is a duplex configuration, configure the **eth2** fields.
5. Verify that you can gain access to Communication Manager using the Out-of-Band Ethernet interface.

   Important:

   You must be able to gain access to Communication Manager using the Out of Band Management Ethernet interface before you perform the next step.
6. Add a static route between the Out of Band Management interface and the enterprise network.

   You must ensure that you add a static route between the Out of Band Management interface and the enterprise network to restrict access. For more information, see “Add a static route between the Out of Band Management interface and the enterprise network”.

7. From the **Restrict Management traffic to Out-of-Band interface is currently** drop-down list, select **enabled**.

Note:

Restrict Management traffic to Out-of-Band interface is set to **enabled**. **Restrict Management traffic to Out-of-Band** will restrict traffic on ports 80, 443, 22, 2222, 5022, 23, 5023, 161, and 162 to the management interface only.

Port restriction

When the **Restrict Management traffic to Out-of-Band** field is set to **enable**, the system restricts traffic on the following ports:

Port	Use
22	ssh
23	telnet
80	http
161	snmp
162	snmp trap
443	https
2222	high priority ssh
5022	sat over ssh
5023	sat over telnet

Adding a static route between the Out-of-Band management interface and the enterprise network

About this task

Create a static route between the Out-of-Band management interface and the enterprise network to route all management functions data through the Out-of-Band management interface.

Procedure

1. Log in to Communication Manager SMI.
2. Click **Administration** > **Server (Maintenance)**.
3. In the navigation pane, click **Server Configuration** > **Static Routes**.
4. Configure the following fields:
   - **IP Address**: Enter the enterprise network IP address.
   - **Mask / Prefix**: Enter the subnetwork mask of the network IP address.
   - **Gateway**: Enter the gateway address.
   - **Interface**: Select **eth1**. If the Communication Manager instance is a duplex configuration, select **eth2**.

5. Click **Add Route**.

Chapter 138: Overriding of SAC/CF

Use the Send All Calls and Call Forwarding (SAC/CF) Override feature to override active rerouting. You can also protect groups of users using this feature. It overrides these active rerouting settings:

- Send All Calls (SAC): Redirects all calls to any administered extension.
- Call Forwarding (CF) all: Forwards all calls to any adminstered extenstion, off-network or attendant group.
- Enhanced Call Forwarding (ECF) unconditional: Forward incoming calls to different destinations depending on whether they are from internal or external sources.

The Overriding of SAC and CF feature is a standard feature starting with Communication Manager Release 5.2.

From Communication Manager Release 5.1 onwards, you can activate the Team Button feature to use its speed dial function and to override a rerouting caused by active SAC, CF, and ECF. For more information, see Team Button on page 1300.

Detailed description of Overriding of SAC/CF

Enabling the SAC/CF override feature depends on call initiation. Call using the dial pad (dialing) or using the Priority button. On enabling SAC/CF override, the call may:

- Execute override – Ring called station
- Execute no override – Forward the call to the coverage or forwarding destination
- Display message – Wait for further input

The settings controlling SAC/CF override are listed here:

Class of Restriction (COR) settings:

- COR of calling station – SAC/CF Override by Dialing
- COR of calling station – SAC/CF Override by Priority button
- COR of called station – SAC/CF Override Protection

Station screen:

- Calling station screen: SAC/CF Override

Overriding of SAC/CF administration

Enable overriding by administering the settings on the Class of Restriction screen (COR), Systems Parameters and the corresponding calling station screens. These settings enable a user at the calling station to override active rerouting.

- Set SAC/CF Override by Dialing on the Class of Restriction screen (COR).
- Set SAC/CF Override by Priority Call on the COR screen.
- Set SAC/CF Override Protection for Dialing on the COR screen of the called station to disable SAC/CF Override by Dialing Call for the calling station.
- Set SAC/CF Override Protection for Priority Calls on the COR screen of the called station to disable the SAC/CF Override by Priority Call setting.
- Specify permissions to allow or restrict call override by selecting ask / no / yes on the Station screen.

The settings on the Station screen of the monitoring station are:

- no - cannot override rerouting. The station doesn't have the ability to override rerouting.
- yes - can override rerouting. The station can override the rerouting the called station has set, provided one incoming call appearance is free and the called station can override by its COR settings. If no free call appearance is available or protection is set, the call fails and the user of the monitoring station hears busy tone.
- ask - ask whether the user wants to follow the rerouting or override it. When the user of the station can decide whether rerouting should take place or not, a message is sent to the station which displays the active rerouting and the number of the forwarded station. The user of the monitoring station can now follow the rerouting by dialing 1 or #, or by letting the timer which supervises the team button pushes expire, or overriding the active rerouting by dialing 0 or *.

Related links

Enabling SAC/CF Override by Dialing or Priority calling on page 1090
Enabling SAC/CF Override Protection on page 1091
Enabling SAC/CF Override for station with or without display on page 1091

Enabling SAC/CF Override by Dialing or Priority calling

Procedure

1. Enter `change cor`.
2. Set the **SAC/CF Override by Dialing** field to `y` to enable the override for dialing.
3. Set the **SAC/CF Override by Priority Call** field to `y` to enable the override for priority calling.
4. Select **Enter** to save your changes.

Note:

SAC does not apply on priority calls. Changing **SAC/CF Override by Priority Call** field on the COR form does not affect SAC, however it enables you to override the call-forwarding feature.

Enabling SAC/CF Override Protection

Procedure

1. Enter `change cor`.
2. Set the **SAC/CF Override Protection by Dialing** field to `y` to enable the override protection by dialing.
3. Set the **SAC/CF Override Protection by Priority Call** field to `y` to enable the override protection by priority call.
4. Select **Enter** to save your changes.

Enabling SAC/CF Override for station with or without display

Procedure

1. Enter `add station` or `change station`.
2. In the **SAC/CF Override** field, enter `y` to enable the override or enter `ask` to see message on a station with display.
3. Select **Enter** to save your changes.

SAC/CF Override operation

SAC/CF Override conditions

COR of calling station: SAC/CF Override by Dialing/Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional settings	Notes/Results
yes	no	ask	Call Forward Override on System Parameters screen Call Coverage/Call Forwarding is set to y.	Dialed call overrides SAC/CF unconditionally without asking when the call is forwarded back to the calling station.
yes	no	ask	Call Forward Override on System Parameters screen Call Coverage/Call Forwarding is set to y.	Priority button call overrides SAC/CF unconditionally without asking.
yes	no	yes / ask	NA	Priority button call overrides SAC/CF unconditionally. Active rerouting enabled at principal station. (CF all or ECF unconditional are active.) **Note:** This case is the standard override case.
yes	no	yes / ask	NA	Dialed call or Priority button call overrides SAC/CF. User at called station picks up the call.

Table continues…

COR of calling station: SAC/CF Override by Dialing/Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional settings	Notes/Results
yes	no	yes	NA	Dialed call overrides SAC/CF when called station is idle on any last call appearance.
yes	no	yes	NA	Priority button call overrides SAC/CF when called station has at least one call appearance available.
yes	no	yes	NA	Dialed call or Priority button call overrides SAC/CF at called station with active auto answer. Auto answer is unexecuted.
yes	no	yes	NA	Dialed call or Priority button call overrides SAC/CF. The Reset Shift Call function is unexecuted at called station.
yes	no	yes	NA	Dialed call or Priority button call overrides SAC/CF. Overriding precedes station hunting at called station.

Ask for SAC/CF Override conditions

COR of calling station: SAC/CF Override by Dialing/Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes/Results
yes	no	ask	Call Forward Override on System Parameters screen Call Coverage/Call Forwarding is set to n.	Dialed call results in a message displayed at calling station.

Table continues…

COR of calling station: SAC/CF Override by Dialing/Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes/Results
yes	no	ask	Call Forward Override on System Parameters screen Call Coverage/Call Forwarding is set to n.	Active rerouting enabled at principal station. Priority button call results in a message displayed at calling station.
yes	no	yes/ask	All Inside Call in coverage path on called Station screen is set to n.	Rerouting is set to ask. Dialed call results in system displaying a message at calling station. Coverage is disabled.
yes	no	ask	NA	Dialed call results in a message displayed at calling station. Called station has restricted last call appearance. There is no impact of this feature when called station is in idle state. Otherwise the called station is busy.
yes	no	ask	NA	Dialed call results in a message displayed at calling station. The called station has at least one last call appearance available.

Table continues…

COR of calling station: SAC/CF Override by Dialing/Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes/Results
yes	no	ask	NA	Priority button call results in a message displayed at calling station. The called station has at least one last call appearance available.
yes	no	ask	NA	Dialed call or Priority button call result in a message displayed at calling station. The call is forwarded or rerouted.
yes	no	ask	NA	Dialed call or Priority button call result in a message displayed at calling station. Internal auto answer function is unexecuted at the called station.

Call flow when calling phone has SAC/CF override set to ask

About this task

Call by dialing, pressing the dial button or initiating the call from the dial pad.

A message is displayed, informing about the rerouting or overriding. Dialing or pressing any other button leads to the result as follows:

Procedure

1. Dial 0 or # to override the call forwarding within 9 seconds to ring principal station.
2. Dial 1 or * to enable call forwarding or proceed with the call.

No SAC/CF Override conditions

You can prevent SAC/CF from being overridden by enabling **SAC/CF Override Protection** in the COR of the called station. The following table lists the other cases when SAC/CF Override does not apply:

COR of calling station: SAC/CF Override by Dialing/Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes/Results
yes	no	yes/ask	NA	Dialed call or Priority button call results in no overriding of SAC/CF when Group calls are enabled.
yes	no	yes/ask	NA	Dialed call or Priority button call results in no overriding of SAC/CF when Goto Cover is active.
yes	no	yes	NA	Dialed call results in no overriding of SAC/CF when the called station has at least one busy last call appearance.
yes	no	yes	NA	Priority call results in no overriding of SAC/CF when the called station has at least one busy last call appearance.
yes	no	yes	NA	Dialed call or Priority button call results in no overriding of SAC/CF when Do not Dial is active.
yes	no	ask	NA	Dialed call or Priority button call results in no overriding of SAC/CF when Do not Dial is active.

Table continues…

COR of calling station: SAC/CF Override by Dialing/Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes/Results
yes	no	yes	NA	Dialed call or Priority button call results in no overriding of SAC/CF when active rerouting is located in another switch connected through QSIG. The call is rerouted.
NA	NA	NA	NA	Dialed call or Priority button call results in no overriding of SAC/CF when calling station is off-PBX. The call is rerouted.
yes	no	ask	NA	Dialed call or Priority button call results in no overriding of SAC/CF with chained routing active. A message is displayed at the calling station.
yes	no	ask	NA	Dialed call or Priority button call results in no overriding of SAC/CF when Do not Disturb is active. **Note:** This feature is not the same as the SAC/CF override feature.

Table continues…

COR of calling station: SAC/CF Override by Dialing/Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes/Results
NA	NA	NA	NA	Dialed call or Priority button call results in no overriding of SAC/CF for intercom calls enabled at the called station.
NA	NA	NA	NA	Dialed call or Priority button call results in no overriding of SAC/CF for whisper page calls.

Chapter 139: Personal Station Access

A user can activate the Personal Station Access (PSA) feature to associate the preferences and permissions of the user telephone with another telephone of the same type.

Detailed description of Personal Station Access

With the PSA feature, users can associate the preferences and the permissions of the user telephone with another telephone of the same type.

Telecommuting with PSA

With PSA, different users can use the same group of telephones at different times. For example, several telecommuting users can use the same office on different days of the week. The users use PSA to associate with the office telephone. When a user associates the telephone, the telephone is assigned to that user. For example, the user can originate and receive calls.

At home, a telecommuting user can also use PSA to install a digital communications protocol (DCP) telephone and a DEFINITY Extender. The user can then call into the system, and use PSA to associate the home telephone with the extension that is assigned to the user at the office. When someone calls the user extension, the call rings at the home of the user.

When a user no longer wants to use PSA, the user disassociates from the telephone.

PSA requires a user to enter a security code, from either an onsite or an off-site telephone.

Invalid attempts to use PSA

Invalid attempts to use PSA generate referral calls. If the Security Violation Notification (SVN) feature is enabled, the SVN software logs the invalid attempt. If a user hangs up, or presses the release button, the system does not log the action as an invalid attempt.

Preferences and permissions with PSA

The preferences and the permissions that are assigned to the user extension, and that are retained with PSA include:

- The definition of terminal buttons
- Abbreviated dial lists

- Class of Service (COS) permissions
- Class of Restriction (COR) permissions

Extensions that do not have a COS, such as expert agent selection (EAS) agents or hunt groups, cannot use PSA.

Button mapping for PSA

PSA functions only on analog, hybrid, and digital communications protocol (DCP) telephones. Many types of DCP telephones exist, with different types and numbers of buttons. If you attempt to associate a DCP telephone or a hybrid telephone with a telephone that has incompatible buttons, button mapping is unpredictable. If you want the user to be able to use the terminal buttons and to have consistent displays, associate stations with terminals of the same type. Telephones and ports on different media servers or switches cannot be associated through PSA. Telephones on different switches, or nodes, within Distributed Communications Systems (DCS) cannot be associated through PSA. The system does not limit the number of stations that can use PSA. However, heavy use of the associate and dissociate functions can have a temporary impact on system performance.

Unanswered calls with PSA

When a call goes to coverage from a PSA-disassociated extension, the software sends a message to the coverage point to indicate that the call was unanswered. If the coverage point is a display telephone, the system displays the letter a which means “don't answer.” If the coverage point is a voice messaging system, the voice messaging system receives an indication from the software that the call was unanswered, and the voice messaging system processes the call as unanswered.

Dissociated telephones with PSA

When a user requests to associate a telephone with PSA, any other telephone that uses the extension is automatically dissociated. Users can place emergency calls from a dissociated telephone, if a COR is assigned to dissociated telephones on the Feature-Related System Parameters screen.

Wit PSA, a bridged appearance can make a dissociate request. However, the system dissociates the telephone from which the user issues the PSA command, even if the user is on a bridged appearance of another telephone.

With the dissociate function within PSA, a user can restrict the features that are available at a telephone. When a user uses PSA to dissociate a telephone, the telephone can only be used to:

- Call an attendant
- Accept a terminal translation initialization (TTI) or a PSA request

To enable users to make other types of calls from dissociated telephones, you must establish a COR for the telephones.

For example, assume that extension 4001 and extension 4002 are administered on telephones A and B. On telephone A, user 4001 dials PSA Associate Code, followed by the extension and security code of user 4002, the following events occur:

- Telephone A associates with extension 4002
- Extension 4001 turns to an AWOH extension (X-port)
- Telephone B is unavailable

When user 4002 dials PSA Dissociate Code on telephone A, the following events occur:

- Telephone A dissociates from extension 4002 and is unavailable
- The dissociation telephone does not restore any previous association with other telephones.
- Extension 4002 dissociates from telephone A and turns to an AWOH

If you again decide to associate these telephones with the same or different extensions, for analog or digital telephones you must use the PSA or TTI feature to associate with an extension and for IP (h.323) telephones you login with an extension.

PSA Security

Security alert:

Once an extension is associated with a telephone, users of that telephone have the capabilities that are associated with the extension. You must issue a dissociate command from the telephone to ensure that unauthorized users cannot use the telephone. Dissociate the telephones if you use PSA and DCP extenders to permit remote DCP access.

Personal Station Access administration

The following task is part of the administration process for the Personal Station Access feature:

- Creating a Feature Access Code for PSA

Related links

Creating a Feature Access Code for PSA on page 1102

Preparing to administer Personal Station Access

Procedure

1. Enable the Personal Station Access feature on your system.
2. Create a class of service (COS) that enables your users to use the capabilities associated with the Personal Station Access feature.

   For more information on how to create a COS, see *Administering Avaya Aura® Communication Manager*.

Screens for administering Personal Station Access

Screen name	Purpose	Fields
Class of Service	Assign PSA to a Class of Service (COS).	Personal Station Access
Feature Access Code (FAC)	Define a Feature Access Code (FAC) to associate and dissociate telephones.	Personal Station Access (PSA) Associate Code and Dissociate Code
Feature-Related System Parameters	Specify the Class of Restriction (COR) to apply to calls made from dissociated telephones.	COR for PSA Dissociated Sets
	Specify the calling party number or automatic number identification (ANI) for calls that are made from dissociated telephones.	CPN, ANI for PSA Dissociated Sets
	Specify that the system record PSA transactions in the history log.	Record CTA/PSA/TTI Transactions in History Log?
	The field **Hot Desking Enhancement Station Lock** on the System-Parameters Features screen controls the feature	Hot Desking Enhancement Station Lock
Station	Define the Station Security Code (SSC) for the extension.	Security Code

Creating a Feature Access Code for PSA

Procedure

1. Enter `change feature-access-codes`.
2. Click **Next** until you see the **Personal Station Access (PSA) Associate Code** field.
3. In the **Personal Station Access (PSA) Associate Code** field, type an FAC for a user to associate a telephone.
4. In the **Personal Station Access (PSA) Disssociate Code** field, type an FAC for a user to dissociate a telephone.

   To type an FAC in the **Personal Station Access (PSA) Disssociate Code** field, the **Personal Station Access (PSA)** field in the System Parameters Customer-Options screen must be set to y.
5. Select `Enter` to save your changes.

End-user procedures for Personal Station Access

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Using the PSA associate command

About this task

To use the PSA associate command, perform the actions shown in the table on page 1103.

Table 85: PSA associate commands

Step	User action	System response	Result
1	Dial the Feature Access Code (FAC) for PSA associate.	Dial tone	The request is successful.
		Intercept tone	• The request is unsuccessful, because the request was not made at an analog, a hybrid, or a DCP telephone. • The request is unsuccessful because the telephone is associated with or assigned to a station that does not have PSA permission in its COS.
2	Dial an extension, and then press #.	No response	If the user is at a telephone with a display, this pound sign (#) is the last character that the system displays until the PSA sequence is complete.
3	Dial the Station Security Code (SSC) for the user extension, and then press #.	Confirmation tone	The command sequence is successfully complete. The system queues the request.
		Intercept tone immediately after the confirmation tone.	The request is unsuccessful, because: • Terminal translation initialization (TTI) is disabled for voice. • Either the dialed extension or the originating extension has an add, a change, or a remove action in progress. • You dialed more than 15 digits before you pressed #. Issue the PSA request again.

Table continues…

Step	User action	System response	Result
		Intercept tone	The request is unsuccessful because: • The extension and the SSC are incompatible. - The extension is invalid. - The SSC is invalid for the extension. - Both the extension and the SCC are invalid. The Security Violation Notification (SVN) feature logs this unsuccessful use of PSA as an invalid attempt. • The Class of Service (COS) of the extension does not allow PSA. • An extension in one tenant partition cannot be associated with a telephone in another tenant partition.
		Reorder tone	The request is unsuccessful because: • The extension that was entered is in use. • An agent is logged in at the dialed extension. • The system load is too heavy for the request to occur. The user can try again later.

Interrupting the PSA associate command sequence

About this task

If you enter incorrect information after you enter the FAC, you can interrupt the command sequence and begin again.

Procedure

1. Press * at any time before you press # for the second time.

   The system generates dial tone.

2. Dial the extension, but do not dial the FAC again.

   SVN does not record the interrupted command sequence as an invalid attempt.

Using the PSA dissociate command

Procedure

Enter the FAC for PSA dissociate.

The system responds with confirmation tone, if the:

- System successfully dissociates the telephone

- Telephone was not previously associated

The system responds with intercept tone if the COS of the telephone extension does not use PSA.

Interactions for Personal Station Access

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

Adjunct/Switch Application Interface (ASAI)

You cannot use PSA on an ASAI link, because ASAI uses a Basic Rate Interface (BRI) port. Do not assign a Class of Service (COS) that uses PSA to an ASAI link.

Bridged Appearance

When you issue a PSA dissociate request for the principal telephone, the bridged appearances of the telephone remain active. The bridged appearances remain active if the telephones on which the bridged appearances appear have not been dissociated.

When a call is made to the principal extension, any of the bridged appearances can alert. If the call cannot alert at a bridged appearance of the principal extension, the system routes the call to the coverage path of the principal extension.

Using PSA you can dissociate request from a bridged appearance. However, the system dissociates the telephone at which the user issues the PSA command, even if the user is on a bridged appearance of another telephone.

Call Management

A PSA dissociate request automatically logs out an Automatic Call Distribution (ACD) agent.

Coverage

PSA does not change coverage path operations. If a station is dissociated, the system routes calls to coverage, unless the calls are forwarded.

Property Management System (PMS)

Do not assign a COS that uses PSA to an extension that is assigned to a room, instead of to a user.

Save Translations

PSA commands cannot be run successfully during a save translations operation. When a reset 3 or greater (reset 4, reset 5, and so on) occurs on the system, all associations revert to the state as of the last save translations operation.

Security Violation Notification (SVN)

If SVN is active, SVN tracks and reports PSA security violations.

Tenant Partitioning

If a telephone is already associated, a user who attempts a PSA associate request at that telephone must specify an extension that is in the same partition as the extension that is already associated with the telephone.

However, any user in any partition can issue a PSA dissociate request at the telephone, if the COS of the telephone extension uses PSA. After the user successfully dissociates the extension, the user can issue a PSA associate request for an extension in any tenant partition.

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.

Chapter 140: Personalized Ringing

Use the Personalized Ringing feature to hear one of eight ringing patterns for incoming calls. You assign the ringing pattern to each user on your system. The different ringing patterns help users who work in the same area to distinguish their calls from the calls of other users.

Detailed description of Personalized Ringing

You can administer Personalized Ringing for each telephone. Either you, or the end user, can administer Personalized Ringing for some programmable telephones.

Personalized Ringing Ringing patterns

The eight administrable ringing patterns are different combinations of three tones. The eight tone combinations are (in Hertz):

- 750, 750, 750 (standard ringing)
- 1060, 1060, 1060
- 530, 530, 530
- 530, 1060, 1060
- 1060, 1060, 530
- 1060, 530, 530
- 1060, 530, 1060
- 530, 1060, 530

Power failures with Personalized Ringing

The user-specified ringing pattern for some digital telephones is lost when the power fails. The system retains the user-specified ringing pattern for ISDN-BRI telephones when the power fails.

Personalized Ringing administration

The following task is part of the administration process for the Personalized Ringing feature:

- Assigning Personalized Ringing to a user telephone

Related links

Assigning Personalized Ringing to a user telephone on page 1108

Screens for administering Personalized Ringing

Screen name	Purpose	Fields
Station	Assign Personalized Ringing to a user telephone.	Personalized Ringing Pattern

Assigning Personalized Ringing to a user telephone

Procedure

1. Enter `change station n`, where *n* is the user telephone to which you want to assign Personalized Ringing.
2. In the **Personalized Ringing Pattern** field, type one of the valid entries shown in the table on page 1108.

   Use the following key to the Usage column:

   - L - 530 Hz
   - M - 750 Hz
   - H - 1060 Hz

   For virtual stations, the **Personalized Ringing Pattern** field dictates the ringing pattern on the mapped-to physical telephone.

   Table 86: Personalized ringing patterns

Valid entries	Usage
1	MMM (standard ringing)
2	HHH
3	LLL
4	LHH
5	HHL
6	HLL
7	HLH
8	LHL

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

Interactions for Personalized Ringing

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

Distinctive Ringing

With Distinctive Ringing, you can administer the relationship between the number of ring bursts and the call type. The Personal Ringing Pattern that you select is the same ringing pattern that is used in the Distinctive Ringing cycles.

Chapter 141: PIN Checking for Private Calls

Use the PIN Checking for Private Calls feature to include three new Feature Access Codes (FACs) providing General, ARS (External) and AAR (Internal) access codes.

For example:

- General operation: *11 12345 04069204130
- External operation: *12 12345 9 04069204130
- Internal operation: *13 12345 04069204130

Detailed description

The PIN Checking for Private Calls feature restricts users from making private calls (internal or external) by forcing them to enter a Personal Identification Number (PIN) code after dialing PIN Feature Access Code. When the PIN is valid, user can dial the destination digits to make a call. The PIN code used for the call is reported in Call Detail Record (CDR) output with a special character P.

The PIN code access feature works in the following way:

1. User dials new Feature Access Code (FAC) administered for this feature.
2. Confirmation tone is played if the FAC dialed by user is valid. On telephone sets supporting displays, user is prompted by message `ENTER PIN`.
3. After user dials an Assigned PIN Code and, if the code is accepted, then user gets recall dial tone on the telephone to enter destination digits. `ENTER NUMBER` message is displayed on telephones that support display.
4. When the feature is invoked by a display equipped DCP or H.323 IP telephone, a character * is displayed for each digit of the PIN code dialed.
5. After entering a destination number the private call can be routed.

Note:

This feature is available with Communication Manager Release 5.2 and later only. This feature does not support IP (SIP) telephones at present.

Making calls using PIN Checking FACs examples

1. PIN Checking for Private Calls Access Code: *11
2. PIN Checking for Private Calls Using ARS Access Code: *12
3. PIN Checking for Private Calls Using AAR Access Code: *13
   - To make outgoing calls from the telephone user needs to follow the following order of using PIN Checking for Private Calls Access Code:

PIN_FAC + PIN_CODE + Destination Digits

*11 + 12345 + 36001

The above Access Code can only be used for internal calls.

- To make external (trunk) calls user needs to use ARS/AAR Access Codes, as shown here:

PIN_FAC + PIN_CODE + Destination Digits

*12 + 12345 + 5400103

PIN_FAC + PIN_CODE + Destination Digits

*13 + 12345 + 5400103

PIN Codes description

This feature reuses the following functionality provided by the Authorization code feature existing in Communication Manager.

Authorization code overrides COR assigned to a station or trunk

Each authorization code is assigned a Class of Restriction (COR). When user dials an authorization code, the COR that is assigned to the extension, the attendant console, the incoming trunk group, or the remote access trunk group that is in use for the call is replaced by the COR assigned to the authorization code. The COR that is assigned to the authorization code functions in the same way as the original COR. However, the new COR that is assigned to the authorization code might represent greater or lesser calling privileges than the original COR. All the parameters on COR screen are applicable to COR assigned to the Authorization code. Access to any given facility depends on the restrictions that are associated with the FRL of the authorization code.

PINs used for this new feature are stored in the same table used by authorization codes. So a PIN has the same COR mapping as authorization codes. See the figure on how PINs are administered on the same screen as Authorization codes. There is no way looking at the administration to distinguish whether particular entry is a PIN or an Auth Code. So, if a user is assigned with some Auth Code, then it can be used instead of a PIN.

```
 change authorization-code 1234567                              Page 1 of 1
                 Authorization Code - COR Mapping
        NOTE: 1      codes administered. Use 'list' to display all codes

      AC       COR         AC       COR         AC       COR         AC       COR
1234567        1
2345678        2
```

Figure 26: Authorization Code Screen

The figure shows administration of a PIN ‘1234567’and an Auth Code ‘2345678’ in same screen. There is no way to distinguish that 1234567 is a PIN and 2345678 is an Auth Code. 2345678 can also be used as a PIN if the COR assigned to that is administered with proper privileges.

Authorization codes length is within 4-13 digit range

The Authorization code feature is enabled in the license file. You can configure the parameters for an Authorization code on the Feature-Related System Parameters screen. For this feature the length of the Authorization code administered on Feature-Related System Parameters screen decides the length of PIN codes. Other fields on system-parameters features screen like, **Authorization Code Cancellation**, **Attendant Time Out Flag**, and **Display Authorization Code** are not applicable to PIN codes.

For security reasons, Communication Manager software requires that authorization codes must consist of 4 to 13 digits. The number of digits in the codes must be a fixed length for a particular server that is running Communication Manager. You can lengthen the authorization code without deleting and reentering the old codes but you cannot shorten the length unless you delete and reenter the old codes. All authorization codes that are used in the system must be the same length. PINs assigned to users for making private calls are of the same length as authorization codes.

Administering PIN Codes

Procedure

1. Enter `change system-parameters features`.
2. In the **Authorization Code Enabled** field, type `y`.

   This enables the Authorization Codes feature on a system-wide basis.
3. In the **Authorization Code Length** field, type the authorization code length.

   This defines the length of the Authorization Codes users need to enter. To maximize the security of user’s system, Avaya recommends making each authorization code the maximum length allowed by the system.
4. 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 user can enter an authorization code.
5. 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.

6. In the **Display Authorization Code** field, type `n`.

   This prevents the authorization code from displaying on telephone sets thus maximizing security.

7. Select **Enter** to save changes.

Enabling PIN Checking for Private Calls

Procedure

1. Enter `change system-parameters features`.
2. Set the **PIN Checking for Private Calls** field to `y`.
3. Select **Enter** to save changes.

Interactions for PIN Checking for Private Calls

Call Detail Recording

The Feature Access Codes (FAC) for **`PIN Checking For Private Calls Access Codes`** with AAR and ARS, and the **`PIN Checking For Private Calls`** are stored along with the PIN Code in the Call Detail Record. Also, a condition code “P” is added to distinguish call dialed using PIN FAC calls. The Call Detail Recording feature reuses the code-dial field. This field stores the ARS FAC, AAR FAC, or TAC. This feature replaces these FACs with the PIN FAC.

Chapter 142: Posted Messages

Use the Posted Messages feature to provide callers with a displayed message on the telephone that states why the user is unavailable to take a call.

Detailed description of Posted Messages

The Posted Messages feature is available with Communication Manager Release 1.3 (V11) or later.

A user activates the Posted Messages feature to post a message to his or her telephone. When a person calls that user, the telephone display of the caller shows the posted message for 4 seconds. During those 4 seconds, the telephone of the caller does not display an incoming call alert. After 4 seconds, the telephone display of the caller reverts back to the normal called number and called name.

To use the Posted Messages feature, the telephone of the caller must be able to display messages. Only internal callers can post or view a posted message. Callers from outside your system cannot view a posted message.

Language options for Posted Messages

Five languages are available for the Posted Messages feature:

- English
- Italian
- French
- Spanish
- A user-defined language

The 15 fixed messages and the feature button labels are available in English, with predefined Italian, French, and Spanish translations. The administrator cannot change the text of the English, the Italian, the French, or the Spanish fixed messages or feature button labels.

The administrator can translate the fixed messages and feature button labels into a user-defined language. This translation can be any other language that you choose, such as German. The administrator can use only one user-defined language throughout the system.

You can administer the 15 custom messages in English, Italian, French, Spanish, and the user-defined language. The number of available messages equals the number of fixed messages (15), plus the number of custom messages that you administer for each language.

Language translation is automatically achieved between telephones and between systems. For example, telephone A uses English and telephone B uses Italian. User A posts the message “In Meeting.” User B calls user A and sees the message “In Riunione” in Italian. If the custom messages are properly administered, the same is true for custom messages.

Messages available with Posted Messages

User can choose from up to 30 different messages. Of these 30 messages, 15 are fixed messages, and 15 are custom messages. Each message has a corresponding message number.

While a user selects a Posted Message, his or her telephone is said to be in selection display mode. Once the user posts a message, his or her telephone is said to be in message posting mode. The telephone screen of the user displays the message. The display of the selected message on the telephone is a visual reminder to the user. The display also indicates the availability of the user to people who might walk into the office.

Telephones that are in message posting mode use a special dial tone when the telephone goes off hook. This special dial tone provides audio feedback to the user. On telephones without a display, this special dial tone is the only indication that the telephone is in message posting mode.

The telephone of the user displays the selected message until:

- The user or someone else deactivates the posted message on the telephone of the user.
- The system resets. If the system resets, the telephone screen of the user no longer displays the posted message.

Posted Messages fixed messages

The numbers for the fixed messages are predefined. You cannot change the numbers or the messages. The following table shows the 15 fixed messages.

Number	Message
01	In Meeting
02	Out To Lunch
03	Away From Desk
04	Do Not Disturb
05	Out All Day
06	On Vacation
07	Gone For The Day
08	Out Sick
09	On Business Trip
10	With Client

Table continues…

Number	Message
11	Working From Home
12	On Leave
13	Back In 5 Minutes
14	Back In 30 Minutes
15	Back In 1 Hour

Note that the Do Not Disturb posted message is independent of the Do Not Disturb feature. Activating or deactivating the Do Not Disturb posted message has no impact on the Do Not Disturb feature.

Posted Messages customer messages

If you choose to add custom messages, you must start with number 16 and continue in numeric order. Custom messages are specific to each local system. Custom messages in any language cannot exceed 28 characters.

QSIG support for Posted Messages

If your system supports QSIG functionality, you can use QSIG to send fixed messages and custom messages to users on other systems. QSIG is a global signaling and control standard for use in private corporate ISDN networks.

The 15 fixed messages are automatically routed to other systems through QSIG. If you want to send custom messages to users on other systems through QSIG, you must:

- Activate QSIG support
- Create the same custom messages on all systems.

  If you do not administer custom messages on the system of the caller, the telephone screen does not display the message of the caller.

Custom messages must be consistent for all systems and for all translations. The reason is that Posted Messages sends the message number, not the message, to the caller. The system of the caller converts the Posted Messages number into a message.

For example, custom message number 16 on system A is “On Conference Call” and custom message number 16 on system B is “Talking to Boss.” If a user on system A posts custom message #16, the user's telephone displays “On Conference Call.” If someone on system B calls the user on system A, Posted Messages sends message number 16 to the caller. The system of the caller converts number 16 into a message. The telephone of the caller displays “Talking to Boss” .

Inconsistent administration on custom messages can display unintended results. The system might not display the intended message.

Posted Messages administration

The following tasks are part of the administration process for the Posted Messages feature:

- Defining a Feature Access Code
- Requiring a security code
- Activating QSIG to send custom messages
- Posted Messages telephone feature button and label translation

Related links

Defining a Feature Access Code for Posted Messages on page 1118
Requiring a Posted Messages security code on page 1119
Activating QSIG to send custom messages on page 1119
Posted Messages translation on page 1120
Posted Messages telephone feature button and label translation on page 1121

Preparing to administer Posted Messages

Procedure

1. Enter `display system-parameters customer-options`.
2. ensure that the **G3 Version** field is set to V11 or later.
3. Click **Next** until you see the **ISDN-BRI Trunks** and the **ISDN-PRI** fields.
4. Ensure that the **ISDN-BRI Trunks** or the **ISDN-PRI** field is set to y, depending on what type of trunk you use.
5. Click **Next** until you see the **Posted Messages** field.
6. Ensure that the **Posted Messages** field is set to y.
7. Click **Next** until you see the QSIG Optional Features screen.
8. Ensure that the following fields are set to y:
   - **Basic Call Setup**
   - **Basic Supplementary Services**
   - **Value-Added (VALU)**

   Note:

   If the **G3 Version** field is not set to V11 or later, and the **ISDN-BRI Trunks**, **ISDN-PRI**, **Posted Messages**, **Basic Call Setup**, **Basic Supplementary Services**, and **Value-Added (VALU)** fields are set to n, your system does not support the Posted Messages feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Posted Messages, or to open a service request.
9. Select **Enter** to save your changes.

Screens for administering Posted Messages

Screen name	Purpose	Fields
Optional Features	Ensure that you have Communication Manager version 1.3 (V11) or later.	G3 Version
	Ensure that your system supports QSIG functionality.	• ISDN-BRI Trunks • ISDN-PRI
	Ensure that the Posted Messages feature is on.	Posted Messages
QSIG Optional Features	Ensure that your system supports QSIG functionality.	• Basic Call Setup • Basic Supplementary Services • Value-Added (VALU)
Feature Access Code (FAC)	Set up a FAC for users to activate and deactivate the Posted Messages feature.	• Posted Messages Activation • Deactivation
Feature-Related System Parameters	Activate QSIG to send custom messages to people on other systems.	Send Custom Messages Through QSIG
	Indicate if users who use a FAC must enter a security code. To activate or deactivate Posted Messages.	Require Security Code
Station	Set up a security code for the telephone of a user.	Security Code
System Posted Messages	Review the 15 fixed messages and, if needed, translate the messages to a user-defined language.	All
Custom Posted Messages	Create or edit up to 15 custom messages in English, Italian, French, Spanish, or a user-defined language.	All
Language Translations	If needed, change the translation of the Posted Messages feature display to a user-defined language.	Posted Messages
	If needed, change the translation of the Posted Messages softkey label to a user-defined language.	PoMsg
	If needed, change the translation of the Posted Messages button label on the 2420 telephone or the 4620 telephone to a user-defined language.	Posted MSGs

Defining a Feature Access Code for Posted Messages

Procedure

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

2. Click **Next** until you see the **Posted Messages Activation** field.
3. In the **Posted Messages Activation** field, type an FAC to activate Posted Messages.
4. In the **Deactivation** field, type an FAC to deactivate Posted Messages.
5. Select **Enter** to save your changes.

Requiring a Posted Messages security code

Procedure

1. Set up a security code for the telephone of a user.
2. Activate the Posted Messages security code.

Setting up the Posted Messages security code

Procedure

1. Enter `change station n`, where *n* is the telephone extension of the user.
2. In the **Security Code** field, type a security code for this telephone.

   The security code can be up to eight digits.
3. Select **Enter** to save your changes.

   Be sure to share this security code with the user.

Activating the Posted Messages security code

Procedure

1. Enter `change system-parameters features`.
2. Click **Next** until you see the **Posted Message** area.
3. Change the **Require Security Code** field to `y`.

   The system displays this field only if the **Posted Messages** field on the Optional Features screen is set to y.
4. Select **Enter** to save your changes.

Activating QSIG to send custom messages

Procedure

1. Enter `change system-parameters features`.
2. Click **Next** until you see the **ISDN Parameters** area.
3. Change the **Send Custom Messages Through QSIG** field to `y`.
4. Select **Enter** to save your changes.

Posted Messages translation

Translating any fixed or custom message to a user-defined language is optional.

To translate Posted Messages, complete the following procedures:

1. Translate fixed messages to a user-defined language.
2. Create customer messages.

Translating fixed Posted Messages

About this task

Fixed messages are available in English, Italian, French, and Spanish. If you want to translate fixed messages into another language, called a user-defined language, complete the following procedure.

Procedure

1. Enter `change display-messages posted-message`.
2. In the **Translation** fields, type a translation of all fixed messages into the user-defined language.

   Note that the text for the English, the Italian, the French, and the Spanish fixed messages are predefined. You cannot change the text of these translations.
3. Select **Enter** to save your changes.

Creating and Translating custom Posted Messages

Procedure

1. Enter `change display-messages posted-message`.
2. Click **Next** until you view the correct screen for the language that you want to use.

   If you first administer custom messages in English, the system displays the text of the English custom messages automatically on the:

   - Italian translations screen
   - French translations screen
   - Spanish translations screen
   - user-defined language translations screen
3. In the **Translation** fields, start with message 16 and type the message in the proper language that you want to create.
4. Continue in numeric order until you create all the custom messages that you want.

   The maximum number of custom messages is 15.
5. Select **Enter** to save your changes.

Note:

Use same instructions to create custom messages in any of the languages.

Posted Messages telephone feature button and label translation

This procedure is optional.

To translate telephone feature buttons and labels for Posted Messages to a user-defined language, complete the following procedures:

1. Translate the Posted Messages feature display to a user-defined language.
2. Translate the Posted Messages softkey button label to a user-defined language.
3. Translate the Posted Messages button label to a user-defined language.

Translating the Posted Messages feature display to a user-defined language

Procedure

1. Enter `change display-messages view-buttons`.
2. Click **Next** until you see the **Posted Messages** field.
3. In the **Translation** fields, type a translated name for Posted Messages into the user-defined language.

   Note:

   The language translations for the English, the Italian, the French, and the Spanish feature display are predefined. You cannot change the text of these translations.
4. Select **Next** to save your changes.

Translating the Posted Messages softkey button label to a user-defined language

Procedure

1. Enter `change display-messages softkey-labels`.
2. Locate the **PoMsg** field.
3. In the **Translation** fields, type a translated name for the PoMsg softkey button label in the user-defined language.

   You are limited to five spaces for this translation.

   Note:

   The language translations for the English, the Italian, the French, and the Spanish softkey button labels are predefined. You cannot change the text of these translations.
4. Select **Enter** to save your changes.

Translating the Posted Messages button label to a user-defined language

About this task

The 2420 DCP telephone and the 4620 IP telephone have digital button labels instead of paper labels. If you need to translate the Posted Messages button labels into a user-defined language for these telephones, follow this procedure.

Procedure

1. Enter `change display-messages button-labels`.
2. Click **Next** until you see the **Posted MSGs** field.
3. In the **Translation** field, type a translated name for the Posted MSGs button label into the user-defined language.

   Note:

   The language translations for the English, the Italian, the French, and the Spanish button labels are predefined. You cannot change the text of these translations.
4. Select **Enter** to save your changes.

End-user procedures for Posted Messages

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

To activate and deactivate the Posted Messages feature, users can either:

- Dial a Feature Access Code (FAC)
- Press a feature button on the telephone

Users can dial the FAC from:

- Their own telephone
- Another telephone on the same system
- A remote access trunk

A user can dial the Posted Messages FAC from another telephone on the same system, and have the message post on their own telephone. Users must press the feature button on their own telephone to activate or deactivate the Posted Messages feature.

To use a FAC to post a message, users might also have to dial the security code for their telephone. The administrator sets up the system to either require or not require a security code. Ask your administrator if you must dial a security code, and what might be the security code for your telephone.

You cannot use the Posted Messages feature from an attendant console. However, you can the Posted Messages FACs to activate or deactivate this feature for other telephones from an attendant console.

Related links

Activating Posted Messages with an FAC on page 1123
Deactivating Posted Messages with a FAC on page 1124
Activating Posted Messages with a feature button on page 1124
Deactivating Posted Messages with a feature button on page 1125

Activating Posted Messages with an FAC

Procedure

1. Dial the FAC for Posted Messages activation.

   You hear dial tone.

2. Identify your extension:
   - If you dial from your own telephone, press #.
   - If you dial from another internal telephone or a remote access trunk, dial your telephone extension. Then press #.
3. Identify the security code for your telephone:
   - If you do not have to dial a security code, press #.
   - If you have to dial a security code, dial the security code for your telephone. Then press #.

     If an error occurs, you hear intercept tone. Press * to clear the extension and security code. Repeat from Step 2. If you do not hear intercept tone, continue with Step 4.
4. Dial the 2 digit number of the message that you want to post.

   Press #.

   You hear confirmation tone. The system posts the message to the telephone display after 1 second as long as the:
   - Telephone does not receive an incoming call
   - User does not press any other button on the telephone

Posted Messages activation examples

You want to post a message to your telephone. For the following examples:

- The activation FAC is *29.
- Your telephone extension is 1234567.
- The security code for your telephone, if needed, is 86562563.
- The message that you want to post to your telephone is message 02, Out To Lunch.

From	Dial
Your own telephone that requires a security code	*29#86562563#02#
Your own telephone that does not require a security code	*29##02#
Another telephone that requires a security code	*291234567#86562563#02#
Another telephone that does not require a security code	*291234567##02#

Deactivating Posted Messages with a FAC

Procedure

1. Dial the FAC for Posted Messages deactivation.
2. Identify your extension:
   - If you dial from your own telephone, just press #.
   - If you dial from another internal telephone or a remote access trunk, dial your telephone extension. Then press#.
3. Identify the security code for your telephone as follows:
   - If you do not have to dial a security code, press #.
   - If you do have to dial a security code, dial the security code for your telephone. Then press #.

     If an error occurs, you hear intercept tone. Press * to clear the extension and security code. Repeat from Step 2.

     If there is no error, you hear confirmation tone. The telephone returns to the normal mode. The system clears the selected message.

Posted Messages deactivation examples

You want to remove the posted message from your telephone. For the following examples:

- The deactivation FAC is #29.
- Your telephone extension is 1234567.
- The security code for your telephone, if needed, is 86562563.

From	Dial
Your own telephone that requires a security code	#29#86562563#
Your own telephone that does not require a security code	#29##
Another telephone that requires a security code	#291234567#86562563#
Another telephone that does not require a security code	#291234567##

Activating Posted Messages with a feature button

Procedure

1. Press the Posted Messages feature button.

You can use this method to post a message only to your own telephone.

2. Use of the following methods to select the message that you want to post:
   - Press the Posted Messages feature button to scroll through the available messages. Whenever you press the feature button, the system displays the next message. To select the message that you want to post, press #.
   - Dial the 2 digit number of the message that you want to post. Press #.

   You hear confirmation tone. The system posts the message to the telephone display after 1 second as long as the:
   - Telephone does not receive an incoming call
   - User does not press any other button on the telephone

Deactivating Posted Messages with a feature button

Procedure

Press the Posted Messages feature button on your telephone.

You can use this method to cancel a posted message only on your own telephone.

You hear confirmation tone. The telephone returns to the normal mode. The system clears the selected message.

Considerations for Posted Messages

This section provides information about how the Posted Messages feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Posted Messages under all conditions.

Performance impact

Heavy use of the selection display mode might adversely affect system performance. Hardware buffers can overflow when you overuse telephone displays. Telephone hyperactivity checks are usually sufficient to control overuse of the display mode.

Security

When a user activates the Posted Messages feature from a remote access trunk, the user must log in as a remote user. When you log in as a remote user, you prevent unauthorized users from activating or deactivating this feature for telephones.

Serviceability

In the selection display mode, the telephone might go out of service if the user scrolls through the displays too quickly. Scrolling through the displays too quickly causes the telephone to be reset. Active calls are dropped. When a 2420, a 4620 or a 4630 telephone is out of service, the system clears the call log.

Time out

If no activity occurs within 60 seconds of the last action, the telephone automatically exits from the selection display mode. The following events occur:

- The LED for the feature button goes out. Or on telephones with feature icons, the feature icon changes to the off state.
- The displayed message is cleared.
- The display of any active call is restored.

When the telephone is in the selection display mode, the timer is reset if a user presses:

- The feature button
- The **Next** button
- Any digit key

Silent ringing

While a telephone is in the message posting mode, the user hears a burst of ringing, and then the telephone rings silently. Silent ringing removes the ringing disturbance while the user can still answer the incoming call.

Interactions for Posted Messages

This section provides information about how the Posted Messages feature interacts with other features in your system. Use this information to ensure that you receive the maximum benefits of Posted Messages in any feature configuration.

Display mode interactions

The system cancels the selection display mode if one of the following telephone display modes is activated.

- Normal

  The normal mode displays call related information for the active call appearance. Depending on the type of call, this information can include the name and the number of the calling party or the called party.

  The elapsed time function can be invoked anytime that the display is in Normal mode. The elapsed time feature displays elapsed time in hours, minutes, and seconds.

- Inspect

  The inspect mode displays call related information for an incoming call when the user is active on a different call appearance. You must reset the mode manually for each call.

- Stored number

  The stored number mode displays one of the following numbers:

  - The last number that the user dialed
  - The number that is stored in an abbreviated dialing button

  - A number that is stored in an abbreviated dialing list
  - A number that is assigned to a button that is administered by the Facility Busy Indication feature
- Date and time

  The date and time mode displays the current date and the time of day.
- Integrated directory

  The integrated directory mode turns off the touchtone signals. A user can activate the integrated directory mode to use the touchtone buttons to enter the name of a system user. After the user enters a name, the display shows the name and the extension.

  Integrated directory mode can also use the **Call-Disp** button. The **Call-Disp** button automatically returns the call that the currently displayed message requested, or by the currently displayed name and extension.
- Message retrieval

  The message retrieval mode retrieves messages for telephone users. If no messages are stored, the display shows NO MESSAGES. A user can retrieve messages even if the user is active on a call.

  Message retrieval mode can use three additional buttons:

  - The Next Message button retrieves the next message. When the telephone is in retrieval mode, the telephone displays END OF FILE, PUSH NEXT TO REPEAT.
  - The Delete button deletes the message that is currently displayed.
  - The Call-Disp button automatically returns the call that the currently displayed message requested, or by the currently displayed name and extension.
- Coverage message retrieval

  The coverage message retrieval mode retrieves messages for users who have telephones without a display. You must administer retrieval permission for a user to retrieve messages from another user.

  The user does not have to lift the handset to retrieve messages. The user can retrieve messages even if the user is active on a call. Coverage message retrieval mode can use three additional buttons:

  - The **Next Message** button retrieves the next message. When the telephone is in retrieval mode, the telephone displays END OF FILE, PUSH NEXT TO REPEAT.
  - The **Delete** button deletes the message that is currently displayed.
  - The **Call-Disp** button automatically returns the call that the currently displayed message requested, or by the currently displayed name and extension.

Diverted Calls

If a user diverts a call to a telephone that is in message posting mode, the calling party does not receive the posted message. For example,

- User A posts a message.
- User B calls user C.

- The system diverts the call through the Call Coverage or Call Forwarding feature to user A.
- User B does not receive the posted message from user A.

Group Extensions, Hunt Groups, Terminating Extension Groups (TEG), intercom groups

The Posted Messages feature does not apply to calls generated from dialing a group extension. The group member remains available to receive calls, and the calling party does not see the posted message.

The Posted Messages feature only applies when dialing the group member's own extension.

No Hold Conference

With No Hold Conference, a user can automatically conference another party while continuing the conversation on the existing call. The new party is automatically added to the existing call upon answer.

If the No Hold Conference feature is in process, the user cannot use the Posted Messages feature. If the telephone is in selection display mode, the user cannot use the No Hold Conference feature.

Personal Station Access/Terminal Translation Initialization (PSA/TTI)

After PSA/TTI dissociation, the extension of the telephone becomes an X-port extension. If the Posted Messages feature was previously activated for the extension, the Posted Messages feature is deactivated.

The permanent display for the Posted Messages feature has precedence over the permanent displays for the PSA enhancements feature:

- if the Posted Messages feature and the Personal Station Access feature are both active
- when the telephone is PSA-associated

Transfer

Under normal conditions, the system displays a posted message only to a calling party. The system does not display a posted message to other parties to whom the call might later be transferred.

The system displays a posted message to the telephones of all transferees if both these conditions apply:

- if a user activates a posted message while the telephone is ringing
- after the transfer operation is completed

Chapter 143: Priority Calling

Use the Priority Calling feature to provide a special type of call alerting between internal telephone users, including the attendant. The called party hears a distinctive ringing when the calling party uses Priority Calling.

Detailed description of Priority Calling

You enable Priority Calling for your system. The Class of Service (COS) that you assign to each user determines whether a user can use Priority Calling.

The following types of calls are always priority calls:

- Call coverage consult
- Automatic callback
- Ringback queuing
- Attendant intrusion
- Security violation notification (SVN)

The system assigns a three-burst ringing-pattern as the default for a Priority Calling call.

The system generates the call waiting ringback tone that a single-line telephone user hears, even if the user is active on a call.

In contrast, the system does not generate the call waiting ringback tone for a multiappearance telephone if no call appearances are idle. Instead, a caller with a multiappearance telephone hears busy tone. The system generates the call waiting ringback tone if the telephone has an idle call appearance, including the call appearance that is reserved for call origination.

Note:

The **VIP Caller** field that is assigned in the Class of Service screen enables automatic priority calling when assigned to the originator of the call. This field might automatically be set to y by the ProVision tool (or any other similar software tool) used by Avaya administration personnel. If stations are set to y, the call will not follow with coverage to voice mail. You must change the setting to the default n to ensure coverage to voice mail.

Priority Calling administration

The following tasks are part of the administration process for the Priority Calling feature:

- Administering Feature-Related System Parameters for Priority Calling
- Creating a Priority Calling Feature Access Code
- Assigning a priority feature button to an attendant console
- Assigning a priority feature button to a telephone

Related links

Assigning a priority feature button to a telephone on page 1131
Assigning a priority feature button to an attendant console on page 1131
Creating a Priority Calling Feature Access Code on page 1131
Administering Feature-Related System Parameters for Priority Calling on page 1130

Preparing to administer Priority Calling

Procedure

Create a Class of Service (COS) that for your users to use Priority Calling.

For more information about how to create a COS, see the Class of Service feature.

Screens for administering Priority Calling

Screen name	Purpose	Fields
Attendant Console	Assign a priority feature button to an attendant console.	Any available button field in the **Feature Button Assignments** area
Class of Service	Define a COS that supports Priority Calling.	Priority Calling
Feature Access Code (FAC)	Define a FAC for Priority Calling.	Priority Calling Access Code
Feature-Related System Parameters	Assign the number of rings for a priority call.	Distinctive Audible Alerting - Priority
Station (multiappearance)	Assign a priority feature button for Priority Calling to a multiappearance telephone.	Any available button field in the **Button Assignments** area

Administering Feature-Related System Parameters for Priority Calling

Procedure

1. Enter `change system-parameters features`.

Note:

The Feature-Related System Parameters screen displays the **Distinctive Audible Alerting** field only when the **Tenant Partitioning** field on the System Parameters Customer Options screen is set to `n`. If the **Tenant Partitioning** field is set to `y`, you must change the **Distinctive Audible Alerting** area on the Tenant screen.

2. Click **Next** until you see the **Distinctive Audible Alerting** area.
3. In the **Priority** field in the **Distinctive Audible Alerting** area, type `priority` next to the number of rings that you want the system to use for a priority call.

   For virtual stations, the number of rings applies to the mapped-to physical telephone.
4. Select **Enter** to save your changes.

Creating a Priority Calling Feature Access Code

Procedure

1. Enter `change feature-access-codes`.
2. Click **Next** until you see the **Priority Calling Access Code** field.
3. Type the FAC that you want to use for Priority Calling.
4. Select **Enter** to save your changes.

   For more information, see the Feature Access Code feature.

Assigning a priority feature button to an attendant console

Procedure

1. Enter `change attendant` *n*, where *n* is the number of the attendant console to which you want to assign a priority feature button.
2. Click **Next** until you see the **Feature Button Assignments** area.
3. Type `priority` next to the feature button that you want the attendant to use for Priority Calling.
4. Select **Enter** to save your changes.

Assigning a priority feature button to a telephone

Procedure

1. Enter `change station` *n*, where *n* is the extension of a multiappearance telephone to which you want to assign a priority feature button.
2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
3. Type `priority` next to the button assignment that you want the user to use for Priority Calling.
4. Select **Enter** to save your changes.

End-user procedures for Priority Calling

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. A user can activate Priority Calling before or after the user places a call.

Activating Priority Calling before placing a call

Procedure

1. Dial the for priority calling Feature Access Code (FAC) and an extension.
2. Press a priority feature button and dial an extension.

Activating Priority Calling after the call starts

Procedure

Press the priority feature button when the call starts to ring at the destination

Considerations for Priority Calling

This section provides information about how the Priority Calling feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Priority Calling under all conditions. The following considerations apply to Priority Calling:

- The Priority Calling feature currently does not work correctly if each of the call's parties is using a SIP endpoint administered on and managed by a different instance of Communication Manager.

Interactions for Priority Calling

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

Abbreviated Dialing

To place a priority call to an extension on an abbreviated dial list, the user must use a button to which both the Feature Access Code (FAC) for Priority Calling and Abbreviated Dialing are assigned.

Call Coverage

The system redirects a call to coverage if the user activates Go to Cover for the call. When the call goes to coverage, the call remains a priority call. The covering user hears the priority call ringing pattern.

Call Forwarding All Calls

The system forwards priority calls, except callback calls. When the system forwards a call, the call remains a priority call.

Call Vectoring

The system generates intercept tone when someone attempts to activate Priority Calling toward a vector directory number (VDN).

Call Waiting

A priority call waits on an active single-line telephone, even if Call Waiting is not assigned to the telephone. The user with an active, single-line telephone who receives the call, hears the distinctive priority Call Waiting tone.

Consult

A Consult call acts as a priority call and waits at a single-line telephone, even if the telephone does not have Call Waiting Indication assigned.

Distributed Communications System (DCS)

With a DCS tandem call to a single-line telephone, the called party does not receive priority ringing, if the caller presses the priority button to activate Priority Calling.

Last Number Dialed

A user must use the Last Number Dialed button to place a priority call to the last number dialed. The Last Number Dialed FAC is invalid after a user activates Priority Calling.

You can administer single-line telephones, for example, 2500-series telephones, so that the system does not provide distinctive ringing. If you administer single-line telephones in this way, the system provides one-burst ringing for priority calls.

Chapter 144: Privacy

Use the Privacy feature to protect your call from interruptions.

Privacy supports the following capabilities:

Data Privacy for voice or data calls

Prevents voice or data calls from being disturbed by any overriding or ringing features

Data Restriction for voice or data calls

Prevents voice or data calls from being disturbed by an overriding or ringing, features or system-generated tones.

Privacy-Automatic Exclusion

Automatically prevents other multiappearance users from bridging onto a call

Manual Exclusion

Prevents other multiappearance users from bridging onto a call when the recipient of the call presses the **exclusion** button

Detailed description of Privacy

Data Privacy

The Data Privacy capability prevents analog data calls from being disturbed by any overriding or ringing features. You administer Data Privacy for each user.

Data Restriction

The Data Restriction capability prevents voice or data calls from being disturbed by any overriding or ringing feature or by system-generated tones. You can administer Data Restriction for either a user or a trunk group. When you administer Data Restriction for a voice telephone, data terminal, or a trunk group, the capability is active for all calls to or from those facilities.

Privacy - Automatic Exclusion

On a multiappearance telephone you can activate Privacy – Automatic Exclusion to keep the participants with appearance of the same extension from bridging on to an existing call. Automatic

exclusion is available as soon as you answer a call. When you press the **exclusion** button to turn off automatic exclusion, place a call on hold and rejoin the call, the exclusion button becomes active again. Simultaneously, other participants with bridged appearance who are active on the call are then dropped from the call.

Privacy - Manual Exclusion

A user of a multiappearance telephone can activate Privacy - Manual Exclusion to keep the participants with appearance of the same extension from bridging on to an existing call. To use manual exclusion, the user presses the **exclusion** button, either before the user places the call, or when the user is active on the call. If the user presses the **exclusion** button while others are bridged onto the call, the system drops the other users. To turn off manual exclusion, the user presses the **exclusion** button.

Privacy administration

The following tasks are part of the administration process for the Privacy feature:

- Administering Privacy for a user
- Activating Data Restriction for a trunk group

Related links

Activating Data Restriction for a trunk group on page 1136
Administering Privacy for a user on page 1136

Preparing to administer Privacy

Procedure

1. Ensure that the **Automatic Exclusion** field on the Feature-Related System Parameters screen is set to y.

   To view the Feature-Related System Parameters screen, enter `change system-parameters features`.

2. Ensure that the **Data Privacy Access Code** field on the Feature Access Codes (FAC) screen is set to y.

   To view the Feature Access Codes (FAC) screen, enter `change feature-access-codes`.

3. Ensure that the **Data Privacy** and the **Automatic Exclusion** fields on the Class of Service screen are set to y.

   To view the Class of Service screen, enter `change cos`.

Screens for administering Privacy

Screen name	Purpose	Fields
Feature Access Code (FAC)	Set the access code for Data Privacy.	Data Privacy Access Code
Feature-Related System Parameters	Activate Privacy-Automatic Exclusion.	Automatic Exclusion by COS.
Class of Service	Enable data privacy for a Class of Service (COS).	Data Privacy
Station	Administer COS.	COS
	Administer an exclusion feature button.	Any available button field in the **Button Assignments** area
	Activate Data Restriction.	Data Restriction?
Trunk Group - all	Activate Data Restriction.	Data Restriction?

Administering Privacy for a user

Procedure

1. Enter `change station n`, where *n* is the extension of the user for whom you want to administer Privacy.
2. In the **COS** field, type the number of the COS that supports Data Privacy.
3. Click **Next** until you see the **Data Restriction?** field.
4. In the **Data Restriction?** field, type `y`.

   If the **Auto Answer** field is set to all or acd, you must not set the **Data Restriction?** field to y.
5. Click **Next** until you see the **Button Assignments** area.
6. In the **Button Assignments** area, type `exclusion` next to the feature button number that you want the user to use activate privacy-manual exclusion, and to deactivate both privacy-manual exclusion and privacy-automatic exclusion.
7. Select **Enter** to save your changes.

Activating Data Restriction for a trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the number of the trunk group for which you want to activate Data Restriction.
2. In the **Data Restriction** field, type `y`.

   Caution:

   Do not change any other fields on this page of the Trunk Group screen without assistance from Avaya or your network service provider.

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

End-user procedures for Privacy

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Using the Privacy feature

Procedure

1. Dial the Feature Access Code (FAC) for Data Privacy at the beginning of the call to activate Data Privacy.
2. Press the **exclusion** button before or during a call to activate Privacy-Manual Exclusion.
3. Press the **exclusion** button to deactivate Privacy-Manual Exclusion or Privacy-Automatic Exclusion.

Considerations for Privacy

This section provides information about how the Privacy feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Data Privacy under all conditions. The following considerations apply to 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 that originate from attendant consoles.
- For virtual extensions, assign the Data Privacy Class of Service to the mapped-to physical extension.
- Do not administer Data Restrictions for an attendant console.

Interactions for Privacy

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

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 that is 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.

When Privacy-Manual Exclusion is active, the system restricts other users to bridge onto the active call.

Busy Verification

Busy Verification cannot be active when Data Privacy is active.

Call Coverage

When the principal user bridges onto a call that has gone to coverage, and the call is answered at the coverage pint, the system does not drop the principal user from the call when Privacy-Manual Exclusion is activated.

Call Pickup

The system does not drop the called party from the call in the following example:

- A call is made to user A.
- User B uses Call Pickup to answer the call.
- User A bridges onto the call by going off-hook on its call appearance.
- User B activates Privacy-Manual Exclusion.

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. This action prevents 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, the multiappearance telephones display Priority Calls on the next available line appearance.

Whisper Paging

If you administer Data Restriction for a telephone, a data terminal, or a trunk group, the system denies Whisper Paging.

Chapter 145: Property Management System Interface

Property Management System (PMS) Interface provides a communications link between Avaya Communication Manager and a customer-owned PMS. A customer can use PMS to control certain features in a hospital and hotel/motel environments. See *GuestWorks® and Avaya MultiVantage™ Enterprise Communications Server Property Management Interface Specifications*.

Detailed description of Property Management System Interface

Table 87: PMS/Communication Manager links on page 1139 summarizes how the hospitality features are activated when you use only Communication Manager and when you use the PMS with Communication Manager.

Table 87: PMS/Communication Manager links

Feature	Communication Manager only	With PMS
Automatic Wakeup	Activated through console button	N/A
Call Coverage	Activated through administration	Activated through PMS terminal — Transparent or ASCII mode
Check-In/Check-out	Activated through console button	Activated through PMS terminal — Normal, Transparent, or ASCII mode
Controlled Restriction	Activated through console button	Activated through PMS terminal — Normal, Transparent, or ASCII mode
Do Not Disturb	Activated through console button	Activated through PMS terminal — Normal, Transparent, or ASCII mode
Emergency Access to Attendant	Activated by guest action	N/A
Housekeeping Status	Activated through console button	Activated through PMS terminal — Normal, Transparent, or ASCII mode
Message Waiting Notification	Activated through console button	Activated through PMS terminal — Normal, Transparent, or ASCII mode

Table continues…

Feature	Communication Manager only	With PMS
Names Registration	Activated through administration	Activated through PMS terminal — Transparent or ASCII mode
Room Change/Swap and Guest Information Input/Change	Activated through administration	Activated through PMS terminal — Normal, Transparent, or ASCII mode
Room Occupancy	Activated through console button	Activated through PMS terminal — Normal, Transparent, or ASCII mode

The PMS Interface provides the following:

- A communications protocol for controlling message exchange between Communication Manager and a PMS
- An application module for controlling the operation of PMS features
- Status data on all guest/patient rooms for selected features

The protocol is full-duplex asynchronous and provides the mechanisms for setting up a data session with PMS, message-exchange control, error identification, and recovery. The interface supports standard data rates.

Two protocol modes are provided: the normal-protocol mode as described above, and transparent-protocol mode. Normal-protocol mode supports a character set that has a combination of Binary Coded Decimal (BCD) characters and ASCII characters. Transparent-protocol mode supports a complete ASCII-character set.

The application module of the PMS Interface implements requested features and provides backup if the PMS link is down. Whether or not the link is down, Communication Manager always maintains the following data for each room:

- Whether the room is vacant or occupied
- Whether the telephone's message lamp is on or off
- Whether a controlled restriction is active at the telephone and, if so, which one
- The guest's name and coverage path

When the PMS link is down, Communication Manager automatically activates Check-In/Check-Out for the attendant console and front-desk terminal with display capability, and continues to support PMS features activated from guest/patient-room telephones.

When the PMS link is up again, Communication Manager sends one of the following messages to PMS:

- No room-status changes occurred during loss of communications.
- Room-status changes did occur during loss of communications; therefore, a data exchange is needed to synchronize Communication Manager and the PMS databases.
- The system failed momentarily, destroying its record of room status; therefore, a data exchange is needed to synchronize Communication Manager and the PMS databases.

When the PMS link is down or not used, Communication Manager maintains an audit-trail report of all events that are normally sent to the PMS. The audit-trail report (accessed via the management

terminal) is a sequential listing of all PMS transactions executed by Communication Manager when the PMS link is down. Included are error events that occur when the link is up or down.

If you have a PMS printer and the PMS link is down, the following status changes print as changes occur:

- Room number
- FAC dialed
- Any additional information digits that were dialed
- Reason for the entry (error message)
- Time that the error occurred

Additional reports print to the PMS Journal/Schedule printer. These include Automatic Wakeup activity, Emergency Access to the Attendant activity, and scheduled reports.

A supporting function called Room Data Image synchronizes Communication Manager and PMS databases after a PMS link goes down and comes back up. Information exchanged includes:

- Room extension
- Whether the room is occupied or vacant
- Message Waiting lamp status
- Controlled Restriction status
- Guest’s name
- Call Coverage path

Message Waiting Notification

Message Waiting Notification requests originate from attendant consoles, front-desk terminals, or PMS terminals. When a request is entered, PMS sends a message to Communication Manager to change the state of the Message Waiting lamp. If the lamp is activated by AUDIX, INTUITY Lodging, or LWC, the PMS cannot deactivate the lamp. PMS cannot turn LWC or AUDIC messages on or off; these are controlled by Communication Manager.

Assign a console permissions COS to any console or terminal as part of the “System Wide Retrieval Stations” to retrieve requests for another station. Assign a client room COS to the extensions for which Message Notification is to be made.

Controlled Restriction

When Controlled Restriction is activated through the PMS, the PMS sends a message to Communication Manager to assign one of the following restrictions to the phone in a guest/patient room:

- No restriction
- Outward restriction

- Total restriction
- Station-to-station restriction
- Termination restriction
- Combined outward and termination restriction
- Combined outward and station-to-station restriction
- Combined termination and station-to-station restriction

The attendant can still set Controlled Restriction for a telephone whether the PMS link is up or down.

PMS-Down Log

The pms-down log records only those User Controller Restriction events that are for stations having a COS where:

- the Client Room field is y
- the Controlled Restriction Configuration field is act-pms
- the pms link is not up
- the pms log extension is valid

Housekeeping Status

Your housekeeping staff enters status information from telephones in guest/patient rooms or from designated terminals. You can assign up to 10 Housekeeping Status access codes within two different types:

- Room telephone access code type

  Staff members dial up to six access codes that represent room status plus up to six additional digits for items such as maid identification.
- Designated telephone access code type

  Staff members dial up to four access codes that represent room status plus the room extension and then up to six additional digits for items such as maid identification.

Communication Manager notifies PMS when Housekeeping Status information is entered. If the PMS is unavailable, Communication Manager writes this information to a log. The log is accessible at Communication Manager system management terminal, and is sent to the log printer, if administered.

Check In/Check Out

A Check-In request deactivates the outward-controlled restriction on the telephone in a guest/patient room. A Check-Out request deactivates any controlled restrictions and changes the controlled-restriction level to outward restriction, checks for any messages, clears the wakeup request, and deactivates Do Not Disturb.

If you do not use PMS or if the PMS link is down, the attendant can activate Check-In and Check-Out from an attendant console or a front-desk telephone with display capability and console

permission. This requires two buttons, Check-In and Check-Out. Pressing either button places the display in the respective mode, and you can use the touch-tone or DTMF buttons for entering data (rather than for placing calls).

The attendant exits Check-In or Check-Out mode by pressing any other button associated with the display (for example, the Normal Mode button). This restores the display and the touch-tone or DTMF buttons to normal operation.

A Check-In/Check-Out request sends information for Names Registration to Communication Manager. This information includes the guest's name, room extension, and call-coverage path. If the PMS link is down and check-in is done from an attendant console or display-equipped front-desk telephone, the guest's name and coverage-path information is manually updated.

If a guest/patient room has both a voice and a data extension, the checkout request applies only to the voice extension.

Room Change/Room Swap

Room Change/Room Swap is provided only through PMS and activated from a PMS terminal. With Room Change, data pertaining to the old room — including a pending wakeup request, the guest's name (transparent/ASCII mode), and the guest's call-coverage path (transparent/ASCII mode) — moves to the new room. With Room Swap, data pertaining to the two rooms swap. With either feature, if the occupancy status is inconsistent, the system sends an error message to PMS.

Names Registration

Names Registration automatically sends a guest's name and room extension from PMS to Communication Manager at check-in, and removes this information at checkout. The guest's call-coverage path is sent to Communication Manager during check-in and set to the administered Default Call Coverage Path for Client Rooms at checkout.

Guest Information Input/Change

Guest Information Input/Change allows the attendant to enter or alter guest information (name or coverage path). Information changed at the PMS is sent automatically to Communication Manager.

PMS/INTUITY Link Integration

With PMS/INTUITY Link Integration, the following PMS administrative messages can tandem through Communication Manager to the INTUITY Lodging adjunct. This eliminates the need for the INTUITY-to-PMS voice messaging link. This does not remove the need for the INTUITY-to-PMS call accounting link.

- Check-in
- Check-out
- Room-data-image (database synchronization)
- Modify (guest-information)

- Add/Remote Text/Fax Notification Message (message-waiting status)
- Transfer/Merge Mailbox (room change/swap)

When the messaging link is down and the PMS/Communication Manager link is up, the Communication Manager buffer holds up to 100 PMS messages. The server updates the INTUITY Lodging adjunct once the link is up. If the buffer overflows before the link is up, the database resync among PMS/Communication Manager/INTUITY initiates by demand or by a routine database update from PMS.

Considerations for Property Management System Interface

This section provides information about how the Property Management System Interface feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Property Management System Interface under all conditions. The following considerations apply to Property Management System Interface:

- You can use Leave Word Calling (LWC) or Integrated Message Center Service for the hospital or hotel/motel staff and Message Waiting Notification for guests/patients. However, if you do not use Message Waiting Notification, Integrated Message Center Service is used for both.
- Do not remove an extension while the PMS link is active.
- With Normal-protocol mode, you can allow extensions of up to four digits. With Transparent/ASCII-protocol mode, you can allow extensions of up to five digits is possible.
- When save translations is done when transparent/ASCII-protocol mode is active, station names with client-room COS save as blank and coverage paths save as the default coverage path for client rooms.
- The PMS link do not work correctly when multiple p-extensions have the same leading digit and adjacent lengths. For example, 3 and 4 p-extensions with the same leading digit may cause problems. The same applies to 4 and 5, and 5 and 6.
- A room extension may begin with 0 only if the PMS sends a prefix digit or a fixed number of digits.

Interactions for Property Management System Interface

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

Attendant Console or Front Desk Terminal

Activate Controlled Restriction, Check-In/Check-Out, and Message Waiting Notification at an attendant console or a front-desk telephone with console permission. The attendant console receives visual notification of the status of the PMS link between the system and the PMS.

AUDIX Interface

Message lamps activated by this feature cannot deactivate with feature buttons or with feature messages from the PMS.

Automatic Wakeup

Set or cancel an Automatic Wakeup request for a guest room as a result of Room Change/Room Swap or Check-Out.

Do Not Disturb

Set or cancel a Do Not Disturb request for a guest room as a result of a different Controlled Restriction, Room Change/Room Swap, or Check-Out.

Leave Word Calling (LWC)

Message lamps activated by this feature cannot deactivate with Manual Message Waiting feature buttons.

If Room Change is active, LWC messages for the old room do not move to the new room. If Room Swap is active, LWC messages for the two rooms do not swap. Therefore, do not encourage use of LWC in guest rooms.

Restriction — Controlled

Controlled Restriction for a group of user extensions, when activated from Communication Manager, is not conveyed to the PMS. The PMS cannot add or remove such restrictions by sending feature messages.

Chapter 146: Provide Agent ID

With the Provide Agent ID feature, an agent endpoint can query Communication Manager and obtain the agent ID once the agent has logged in to the telephone. With the Agent ID, the telephone can query the file server to download applicable greetings files to be played when a call is received. This feature works only with 96x1 H.323 telephones.

Related links

Detailed description of the Provide Agent ID feature on page 1146

Detailed description of the Provide Agent ID feature

In a call center environment, an agent might log in to a telephone by one of the following methods:

- Communication Manager-based feature, such as Abbreviated Dial buttons
- Telephone-based application, such as Contacts
- Computer-based applications

If an agent logs in to a telephone by one of these methods, the telephone might not be able to determine the agent ID. For example, the telephone might not be able to differentiate between the value of the agent ID and the value of the optional password. In case of Computer-based logins, the telephone is out of the loop of the login process, and has no access to the login information.

Without accurate agent ID, the telephone cannot retrieve the Agent Greetings files. The telephone can always determine that the agent is logged in, but cannot always determine the agent ID. If the telephone cannot determine the agent ID, when a customer calls the call center to connect to a specific department, the telephone does not play the proper greeting. Due to these scenarios where the telephone might not be able to determine the agent ID, Communication Manager must send the agent ID to the telephone after the agent logs in.

When the telephone receives a call center event against one of the administered lamps, the telephone initiates an agent ID inquiry message. On receiving the agent ID inquiry message, Communication Manager responds with the agent ID or, if the agent is not logged in, sends a denial event message on the extension of the agent. With accurate agent ID, the telephone can retrieve the specific agent greeting and play the greeting when a call is received.

Related links

Provide Agent ID on page 1146

Chapter 147: Public Network Call Priority

Use the Public Network Call Priority feature to provide call retention, forced disconnect, intrusion, mode-of-release control, and re-ring to servers on public networks.

Detailed description of Public Network Call Priority

Use the Public Network Call Priority feature to provide call retention, forced disconnect, intrusion, mode-of-release control, and re-ring to servers on public networks. Different countries refer to these functions by different names. Not all functions are available in all countries.

China Public Network Call Priority

China forced disconnect

With forced disconnect, a network operator can disconnect a called party from a local call, and connect the called party to an incoming toll call. Parties who are on the local call hear a warning tone before the network operator disconnects the call. Forced disconnect is allowed only for callers on local single-station calls. The system restricts forced disconnect for the following type of calls:

- Conference
- Transferred
- Forwarded
- To group users
- Tandem

China mode-of-release control

Mode-of-release control inhibits release of a trunk circuit when a caller goes on-hook, based on call type and direction. Instead of releasing the trunk circuit, the system keeps the circuit active, and reconnects the call if the caller goes off-hook again. Mode-of-release control applies to the following types of incoming or outgoing calls:

- Toll
- Local

- Service

Public Network Call Priority provides three types of mode-of-release control.

Calling-party control

When calling-party control is active, the trunk is not released until the caller goes on-hook. For example, if the:

- Caller goes on-hook, the trunk is released immediately. The called party receives busy tone.
- Called party goes on-hook, the trunk is not released until the caller goes on-hook, or the re-answer timer for outgoing calls expires. The called party can reanswer the call, and talk to the calling party.

  Re-ring occurs for incoming calls to the system with calling-party control. When the called party goes on-hook, the trunk is not released, and the central office (CO) operator can re-ring the called party and reconnect the call.
- Re-answer timer is activated and expired, the trunk is released on outgoing calls with calling-party control.

Called-party control

When called-party control is active, the trunk is not released until the called party goes on-hook.

- If the called party goes on-hook, the trunk is released immediately, and the caller receives busy tone.
- If the caller goes on-hook, the trunk is not released until the called party goes on-hook. The caller can go off-hook again to reconnect. No timer is involved with called-party control

First-party control

When first-party control is active, the trunk is released immediately regardless of whether the caller or the called party goes on-hook first. The party that is still connected receives busy tone. The default or normal mode-of-release control for the system is first-party control.

Russia Public Network Call Priority

Russia intrusion

A network operator can use intrusion to break into a local call and announce an incoming toll call. Intrusion is allowed on local single-line and multiline telephone calls. The system does not support intrusion for the following types of calls:

- Conference
- On hold
- Toll

Russia re-ring

Re-ring occurs when a call is interrupted by an operator-assisted incoming call, and the call is kept on hold so that the call can be reconnected to a telephone. When the called party goes on-hook, the network toll operator can re-ring the called party, and reconnect the call.

Spain Public Network Call Priority

Spain call retention

When a caller makes an emergency call and then hangs up, the call is put on hold. The system does not disconnect the call. When the caller goes back off-hook, the system reconnects the telephone to the emergency call. Call retention works on both analog and digital telephones.

Spain re-ring

Re-ring occurs when a call is interrupted by an operator-assisted incoming call, and the call is kept on hold so that the call can be reconnected to a telephone. When the called party goes on-hook, the network toll operator can re-ring the called party, and reconnect the call.

Public Network Call Priority administration

This section describes the screens that you use to administer the Public Network Call Priority feature.

Screens for administering Public Network Call Priority

Screens for administering Public Network Call Priority for China

Screen name	Purpose	Fields
Multifrequency-Signaling-Related System-Parameters	Specify the type of tone that is received from a Chinese central office (CO).	Incoming Forward Signal Types for group I and group II
	Specify the type of tone that is sent to a Chinese CO.	Incoming Backward signal Types for group A and group B
Trunk Group	Specify country code 18 for China.	Country
	Specify the outgoing dial type of mf for China.	Outgoing Dial Type
	Specify the incoming dial type of mf for China	Incoming Dial Type

Screens for administering Public Network Call Priority for Russia

Screen name	Purpose	Fields
Trunk Group (DID)	Specify country code 15 for Russia.	Country

Table continues…

Screen name	Purpose	Fields
	Specify the protocol type Intol for Russia.	Protocol Type
Trunk Group (DIOD)	Specify country code 15 for Russia.	Country
	Specify the protocol type Intol for Russia.	Protocol Type

Screens for administering Public Network Call Priority for Spain

Screen name	Purpose	Fields
Trunk Group	Specify country code 11 for Spain.	Country

Interactions for Public Network Call Priority

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

Interactions for Public Network Call Priority for China

China forced disconnect interactions

Conference

If the network toll call terminates at a telephone that is involved in a conference, the network does not send the forced disconnect signal.

Call Forwarding

The system forwards the forced disconnect signal for calls that are forwarded on-premises, on the network, or off the network.

Group Users

The network does not send the forced disconnect signal, if a network toll call terminates to a group user.

Nonstation Users

The network does not send the forced disconnect signal, if a network toll call terminates to a nonstation user. Nonstation users include personal attendant, data module., announcement and voice synthesis users.

Tandem Trunks

The system does not tandem a forced disconnect signal.

Transfer

The network does not send the forced disconnect signal, if a network toll call is transferred.

China mode-of-release control interactions

Conference

A call that is involved in a conference is changed to first-party control as the mode-of-release control.

Forward

A call that is forwarded on-premises, on the network, or off the network is changed to first-party control as the mode-of-release control.

Group users

Group users includes hunt, trunk, terminating extension group (TEG), Communication Manager Messaging, Vector Directory Number (VDN).

Calls that terminate to group users are changed to first-party control as the mode-of-release control.

Nonstation users

Nonstation users includes personal attendant, data-module, announcement, and users of voice synthesis.

Calls that terminate to nonstation users are changed to first-party control as the mode-of-release control.

Tandem Trunks

The system terminates tandem calls, but the mode-of-release control is changed to first-party control.

Transfer

A transferred call is changed to first-party control as the mode-of-release control.

China re-ring interactions

Conference

A call that is involved in a conference is changed to first-party control as its mode-of-release control. first-party control calls do not re-ring.

Call Forwarding

The system does not forward re-ring signals for calls forwarded on-premises, on the network, or off the network.

Group users

Group users includes hunt, trunk, TEG, Communication Manager Messaging, and VDN

The system ignores Re-ring signals that are sent to group users.

Nonstation user

Nonstation user includes personal attendant, data-module, announcement, voice synthesis.

The system ignores Re-ring signals that are sent to nonstation users.

Tandem trunks

The system does not tandem re-ring signals.

Transfer

A transferred call is changed to first-party control as its mode-of-release control. First-party control calls do not re-ring.

Interactions for Public Network Call Priority for Russia

Announcements

The system restricts intrusion and re-ring for an announcement port.

Abbreviated Ringing and Delayed Ringing

Abbreviated Ringing and Delayed Ringing characteristics that you assign do not apply to re-ring. Re-ring has its own priority ringing.

Administered Connections

Intrusion and re-ring do not apply to Administered Connections.

Attendant Console

Intrusion and re-ring do not apply to attendant consoles, or to any call that involves an attendant console.

Attendant Serial Call

The system ignores Intrusion and re-ring for an attendant serial call.

Automatic Callback

Re-ring takes precedence over automatic callback on busy or no-answer calls.

Busy Verification and Attendant Intrusion

While Intrusion or re-ring occurs, Busy Verification and Attendant Intrusion are denied. While Busy Verification or Attendant Intrusion occurs, Intrusion and re-ring are denied.

Call Coverage

Re-ring overrides Call Coverage. However, if a station is busy and a coverage destination is free, an incoming toll call rings at the coverage destination instead of intruding on the busy call.

Call Forwarding

Intrusion can be used with Call Forwarding. If a station is busy, an incoming toll call is forwarded instead of intruding on the busy call. Re-ring overrides all administered redirection.

Call Waiting

If Call Waiting is active, calls are not intruded upon. Call Waiting takes precedence.

Conference

The system restricts intrusion for a call that is involved in a conference.

Data Calls

The system restricts intrusion for telephones that have Data Privacy, Data Restriction, or Data Protection active.

Distinctive Ringing

Ringing characteristics that you assign do not apply to re-ring. Re-ring has its own priority ringing.

Do Not Disturb

You cannot use intrusion and Do Not Disturb at the same time.

Emergency Access to the Attendant

The system restricts intrusion for an emergency call.

Hunt Group and Automatic Call Distribution

If a hunt group queue is not busy, the system places incoming toll calls in the queue. Busy calls are not intruded upon.

Intercom - Automatic and Dial

The system restricts intrusion on any Intercom calls.

Malicious Call Trace (MCT)

The system restricts intrusion on a station that has MCT active.

Personal Station Access (PSA)

The system restricts Intrusion when PSA is in use.

Pull Transfer

The system restricts Intrusion when Pull Transfer is in use.

Class of Restriction (COR)

The system restricts Intrusion, regardless of the COR.

The system supports Intrusion with Ringback Queuing.

Ringback Queuing

Station Hunting

The system supports Intrusion when Station Hunting is used.

Tandem Trunks

The system restricts Intrusion over trunk groups used as tandem trunks.

Chapter 148: 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.

Detailed description of QSIG over SIP

The Q-SIP feature is a mechanism for tunneling QSIG messages over the Session Initiation Protocol (SIP). The Q-SIP feature enables you to:

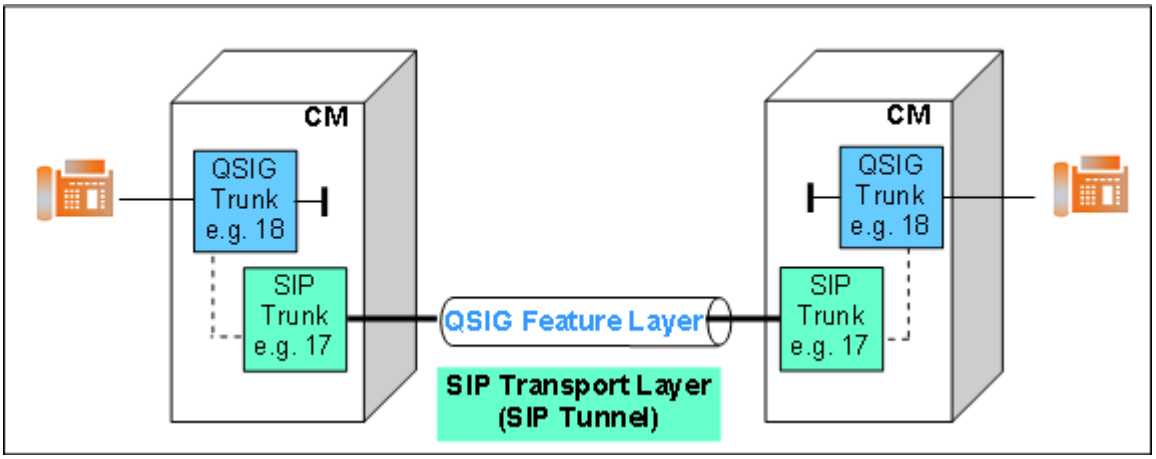
- Use SIP trunking as transport for private networking while maintaining all the QSIG features.
- Migrate from QSIG transported over an ISDN private network to QSIG transported over a SIP network, one-communication system at a time.

There are two layers in Q-SIP:

- A QSIG layer which provides the QSIG features and basic calls.
- A SIP layer which provides transport mechanism.

Each layer has its own trunks.

- QSIG layer— The QSIG trunk is available from the originating device, for example, telephone or trunk. This trunk is used internally to provide the QSIG features and basic calls.
- SIP layer—The SIP trunk provides the transport mechanism for the QSIG features. The SIP trunk connects two Communication Manager nodes.



Both the QSIG and SIP trunks require dedicated signaling and trunk groups. That is, you must configure two trunks and two signaling groups in one Communication Manager to get the Q-SIP feature. Q-SIP reduces the actual trunk pool of the system.

Note:

You need to administer H.323 IP trunks for the QSIG signaling. For information on how to administer H.323 IP trunks, see Administration of the QSIG and SIP trunk and signaling groups.

Note:

As an example the QSIG signaling and trunk group is 18 and the SIP signaling and trunk group is 17. The examples in the following sections refer to these signaling and trunk group numbers.

QSIG over SIP administration

The following tasks are part of the administration process for the QSIG over SIP feature:

- Creating the QSIG and SIP signaling and trunk groups
- Changing the QSIG and SIP signaling groups for Q-SIP
- Changing the QSIG and SIP trunk groups for Q-SIP
- Verifying a Q-SIP test connection
- Disabling Q-SIP for the QSIG and SIP signaling groups
- Disabling Q-SIP for the QSIG and SIP trunk groups

For information on how to administer the above tasks, see *Administering Avaya Aura® Communication Manager*.

Screens for administering QSIG over SIP

Screen name	Purpose	Fields
IP Node Names	Assign an IP address and a name for each node.	Name IP Address
IP Network Region	Assign a domain.	Authoritative Domain

Table continues…

Screen name	Purpose	Fields
Signaling Group	Provide SIP and QSIG signaling groups.	Group Type Max number of NCA TSC Q-SIP QSIG Signaling Group SIP Signaling Group Trunk Group for Channel Selection TSC Supplementary Service Protocol Near-end /Far-end Node Name Near-end /Far-end Listen Port Direct IP-IP Audio Connections
Trunk Group	Provide SIP and QSIG trunk groups.	Group Type Group Name TAC Service Type Signaling Group Number of Members Numbering Format Member Assignment Method Supplementary Service Protocol Digit Handling (in/out) NCA-TSC Trunk Member Send Name Send Calling Number Send Connected Number TSC Method for Auto Callback Enable Q-SIP QSIG Reference Trunk Group SIP Reference Trunk group

Interactions for QSIG over SIP

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

Administer an additional SIP trunk to an existing QSIP trunk

If an additional SIP connection is used between two Communication Managers in parallel to the Q-SIP connection, you must administer a different port for the SIP connection.

Automatic Callback or Call Completion (CCBS/CCNR)

With QSIG, when a CCBS/CCNR request is initiated to a busy or free subscriber, a new TSC connection is established from the originating side. Through the TSC connection, the request is transmitted to the terminating side. The TSC is retained or released, based on the Connection Retention or Connection Released (drop-if-possible) method, and after you enter the request. To avoid TSC with longer duration, use the Connection Released method. With the Connection Retention method, the TSC is up until the CCBS/CCNR request is completed. If the Q-SIP trunk receives a CCBS/CCNR request from a transit PABX, the method chosen by the remote PBX remains unchanged. If you use the Connection Retention method, the method consumes a SIP resource until the CCBS/CCNR request is completed.

Avoid long-term Temporary Signaling Connections for Q-SIP

In Communication Manager, a Temporary Signaling Connection (TSC) is used for a QSIG call-independent (connection oriented) signaling connection. Communication Manager does not support TSC for SIP. Instead, a SIP connection with a SIP resource is established. With Q-SIP a call-independent signaling connection is also transported through a SIP resource. The TSC, which is only a short connection, consumes a SIP resource. If some features maintain a TSC for some minutes and they establish a new TSC for each feature activation, each active TSC reduces the number of available calls over the QSIP trunk. As a longer TSC consumes the SIP resources, you must be careful using features based on a call-independent signaling connection such as Call Completion and Message Waiting Indication.

Call Detail Recording (CDR) records for the QSIG trunks

The QSIG over SIP feature uses two trunks per call, but the system generates Call Detail Recording (CDR) records for the QSIG trunk. To generate the CDR records for the QSIG trunks, you must set the CDR Reports field on the SIP trunk group screen for the Q-SIP pair to n and the CDR Reports field on the QSIG trunk group screen to y.

Compatibility to ECMA-355 (3rd Edition)

Q-SIP is based on ECMA-355 (3rd Edition). Following this Q-SIP standard, Direct Media is not supported.

Inter Gateway Alternate Routing

Inter Gateway Alternate Routing (IGAR) over Q-SIP is not supported in Communication Manager 6.0 release.

Message Waiting Indication (MWI)

Depending on how Message Waiting is configured, Communication Manager sends a REL COMPLETE or a CONNECT message while answering to an incoming MWI request. To avoid

TSC with longer duration, configure Communication Manager to answer with REL COMPLETE. If Communication Manager responds with a CONNECT message, the TSC could stay up for 4 hours: 15 minutes. After this time, Communication Manager releases the connection. If the QSIG part is released, the SIP trunk is also released. You can configure Communication Manager to answer with CONNECT only when the Message Center, which has initiated the MWI request, releases the call with REL COMPLETE after receiving the CONNECT message. For more information, see Configuring message waiting using a QSIG-connected messaging adjunct on page 1158.

Q-SIP queueing on SIP trunk is independent of a Q-SIP call

The Q-SIP queueing on QSIG trunk feature queues calls if the QSIG trunk-group is busy. As soon as a QSIG trunk member becomes available, the call is unqueued and established automatically. The QSIG trunk is used to provide the fundamental mechanism for signaling QSIG messages over SIP.

The Q-SIP queueing on SIP trunk feature cannot work if the SIP trunk-group is busy. Because the SIP trunk is only for the tunnel establishment and provides only the transport mechanism.

Configuring message waiting using a QSIG-connected messaging adjunct

Procedure

1. Log in to the Communication Manager System Administration Terminal (SAT) interface.
2. In the Hunt Group page, navigate to page 2.
3. In the **Message Center** field, enter `qsig-mwi`.

   A new field **TSC per MWI Interrogation?** appears.
4. Depending on the requirements of your messaging adjunct, do one of the following:
   - To have Communication Manager clear TSCs by responding to MWI Interrogations with a Q.931 RELEASE COMPLETE message, enter `Y`.
   - To have Communication Manager keep TSCs active for up to 4¼ hours by responding to MWI Interrogations with a Q.931 CONNECT message, enter `N`. By default, the option is N.

Chapter 149: Recorded Telephone Dictation Access

Use the Recorded Telephone Dictation Access feature to access dictation equipment.

Detailed description of Recorded Telephone Dictation Access

Use the Recorded Telephone Dictation Access feature to access dictation equipment. Users can access the feature from any onsite or off-site telephone, and can use incoming tie trunks to access the feature.

A user enters a Feature Access Code (FAC) or an extension to access the feature. A user can enter commands by key or by voice to control the start and stop functions. A user can enter commands by key to control other functions, such as initial activation.

Recorded Telephone Dictation Access cannot be used with Automatic Route Selection (ARS) or Conference.

For more information, see the following features:

- Audible Message Waiting
- Announcements
- Voice Message Retrieval

Recorded Telephone Dictation Access administration

The following tasks are part of the administration process for the Recorded Telephone Dictation Access feature:

- Assigning manual signaling button to a multiple-call appearance telephone user

Related links

Assigning a signaling button to a multiple-call appearance telephone on page 1160

Screens for administering Recorded Telephone Dictation Access

Screen name	Purpose	Fields
Station	Assign a **signal** button to a user telephone, and specify the extension that rings when the user presses the button.	Any available button field in the **Button Assignments** area

Assigning a signaling button to a multiple-call appearance telephone

Procedure

1. Enter `change station n`, where *n* is the extension to which you want to assign a signaling button.
2. Click **Next** until you see the **Button Assignments** area.
3. Type `signal` next to the number of the button that you want the user to use for manual signaling.

   When you type `signal` next to the button number the system displays an **Ext:** field.
4. Type the extension of the recipient of the signal in the **Ext:** field.
5. Select **Enter** to save your changes.

Interactions for Recorded Telephone Dictation Access

This section provides information about how the Recorded Telephone Dictation Access feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of the Recorded Telephone Dictation Access feature.

Automatic Route Selection (ARS)

You cannot use ARS to access Recorded Telephone Dictation Access.

Conference

You cannot use Conference and Recorded Telephone Dictation Access at the same time.

Chapter 150: Redirect 3PCC to H.323 station from SIP desktop station

Use the Redirect 3PCC to H.323 station from SIP desktop station feature to direct the Third Party Call Control (3PCC) actions to a remote H.323 device.

Detailed description of Redirect 3PCC to H.323 station from SIP desktop station

The Redirect 3PCC to H.323 station from SIP desktop station feature redirects the third-party Call Control (3PCC) actions from a SIP desktop station to one of the following :

- Remote H.323 soft phone
- Virtual private network H.323 telephone

You can enable the feature by activating the **Prefer H.323 over SIP for Dual-Reg station 3PCC Make Call** field or a FAC.

The two FACs that can be used to activate and deactivate the Redirect 3PCC to H.323 station from SIP desktop station feature are:

- **3PCC H323 Override SIP Station Activation**
- **3PCC H323 Override SIP Station Deactivation**

You can start the 3PCC action by using an ASAI 3PCC make call request. If the ASAI link stops working or the station is no longer under domain control, the feature is deactivated.

The computer telephony integration (CTI) application can use any domain-controlled extension to originate the FAC call.

Example of a 3PCC call for dual registration

The following scenario is of a 3PCC call for dual registration when a 3PCC call request comes from an application to an endpoint:

SIP	H.323	Prefer H.323 over SIP for Dual-Reg station 3PCC Make Call is set to no	Prefer H.323 over SIP for Dual-Reg station 3PCC Make Call is set to yes
Registered	Registered	3PCC call originates from SIP.	3PCC call originates from H.323.
Registered	Not registered	3PCC call originates from SIP.	3PCC call originates from SIP.
Not registered	Registered	3PCC call fails.	3PCC call originates from H.323.
Not registered	Not registered	3PCC call fails.	3PCC call fails.

Activating the Redirect 3PCC to H.323 station from SIP desktop station feature by using the system parameters form

About this task

Use the following procedure to start the Redirect 3PCC to H.323 station from SIP desktop station feature without using a FAC.

Procedure

1. Type `change system-parameters features`, and press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. On page 13, in ASAI , set the **Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call** field to `y`.

   The 3PCC actions are redirected from a SIP desktop station to a remote H.323 station.

Activating and deactivating the Redirect 3PCC to H.323 station from SIP desktop station feature by using a FAC

Procedure

1. Type `change feature-access-codes`, and press **Enter**.

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

2. On the Feature Access Code (FAC) screen, do one of the following:

   - To activate the 3PCC redirect actions, enter an activation code in the **3PCC H323 Override SIP Station Activation** field.

- To deactivate the 3PCC redirect actions, enter a deactivation code in the **3PCC H323 Override SIP Station Deactivation** field.

3. To save the changes, press **Enter**.

Viewing the 3PCC redirect action activation and deactivation codes

Procedure

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

   The **3PCC H323 Override SIP Station Activation** field specifies the activation code.

   The **3PCC H323 Override SIP Station Deactivation** field specifies the deactivation code.

2. Click `Enter` to exit the screen.

Interactions for Redirect 3PCC to H.323 station from SIP desktop station

This section provides information about how the Redirect 3PCC to H.323 station from SIP desktop station feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Redirect 3PCC to H.323 station from SIP desktop station in any feature configuration.

Auto Answer

If a station is administered as auto-answer, the H.323 3PCC SIP override feature will not activate on that station.

Chapter 151: Remote Access

Use the Remote Access feature to access and use the system from the public network.

Detailed description of Remote Access

Security alert:

Avaya has designed the Remote Access feature incorporated in this product, when properly administered by the customer, to enable the customer to minimize the ability of unauthorized people to gain access to the network. It is the responsibility of you to take the appropriate steps to properly implement the features, evaluate and administer the various restriction levels, protect access codes, and distribute the access codes only to people whom you advise of the sensitive nature of the access information. Instruct each authorized user to use access codes properly.

In rare instances, unauthorized individuals use the Remote Access feature to make connections to a telecommunications network. In such an event, applicable tariffs require that you pay all network charges for traffic. Avaya cannot be responsible for such charges, and does not make any allowance or give any credit for charges that result from unauthorized access.

The Remote Access caller must access your system from the public network and use a touch tone telephone or equivalent equipment. When a user uses Remote Access, the system does not have access to the calling number, because the calling number is outside the system. Thus, some features and capabilities, such as Ringback Queuing and Automatic Callback, cannot be used on a Remote Access call. Also, the user cannot use any feature that requires recall dial tone, such as, the Hold and Transfer features, from the remote location.

Remote Access provides users with access to the system and system features from the public network. Uses can use Remote Access to make business calls from home or use the Recorded Telephone Dictation Access to dictate a letter. An authorized user can also access system features from any onsite extension.

With Remote Access, you can dial into the system over direct inward dialing (DID), central office (CO), foreign exchange (FX), or 800 service trunks. When a call comes in on a trunk group that is dedicated to Remote Access, the system routes the call to the Remote Access extension that you assigned. If DID is provided, and the Remote Access extension is within the range of numbers that can be accessed by DID, the system uses DID for Remote Access.

You can administer your system so that a user must enter a barrier cod, an authorization code, or both to use Remote Access.

Use barrier codes to secure and define calling privileges through the Class of Restriction (COR) that you administer to users and trunk groups. You can administer as many as 10 barrier codes. Each barrier codes has a different COR and Class of Service (COS). Barrier codes can be from 4 to 7 digits, but all barrier codes that you define must be the same length.

Night Service with Remote Access

You can administer your system to provide attendant-assisted calling during the day, and then Remote Access when the system is in Night Service.

Remote Access Security

To ensure system security, you can permanently disable the Remote Access feature if you do not intend to use the feature. If you permanently disable Remote Access, you must go to the Avaya Support website at http://support.avaya.com to open a service request for activating this feature.

Caution:

Your attempt to disable the Remote Access feature is lost if the server that runs Communication Manager is rebooted without saving translations. Therefore, you must run a **`save translation`** command after you permanently disable the Remote Access feature.

The system provides several ways to secure your system when you use the Remote Access feature:

- The **`status remote-access`** command
- Barrier codes
- Authorization codes
- Alternate Facility Restrictions Levels (AFRLs)
- COR
- Logoff Notification

Status remote-access

You can check the status of the Remote Access feature and the barrier codes. The **`status remote-access`** command displays information that can help you determine when and why the system denied remote access to a user, or why the system blocked a barrier code.

When you type the **`status remote-access`** command, the system displays the:

- Remote Access status:
  - Not administered
  - Enabled
  - Disabled

  - Disabled following detection of a security violation
- Date and time that Remote Access was last modified
- Barrier code information:
  - The date that the code was administered, reactivated, or modified
  - The expiration date
  - The number of calls that can be placed with the code
  - The number of calls that were placed with the code
  - Active or expired status
  - The date and the reason that a code expired

For a detailed description of the **`status remote-access`** command and display, see the *BCS Products Security Handbook*.

Barrier codes with Remote Access

Remote Access has inherent risks, such as large-scale unauthorized long distance use of your telecommunications facilities. To increase the security of your system, use a 7-digit barrier code, and administer expiration dates and access limits for each of the 10 barrier codes that are available to you. If your system has more than 10 Remote Access users, the users must share barrier codes. A barrier code automatically expires if the expiration date or the number of accesses exceeds the limits that you set. You can administer the system to limit:

- The length of time that an access code remains valid
- The number of times that an access code can be used
- Both the length of time that an access code remains valid and the number of times that an access code can be used

When you no longer need a barrier code, remove the code from the system.

If you administer barrier codes, a special answer-back tone causes a calling modem to leave dial mode. Sometimes a modem dialer is used to gain access with Remote Access. When a dialer of a modem is used to gain access with Remote Access, the special answer-back tone cancels echo suppressors on the network. The cancellation of echo suppressors in the network prevents dual-tone multifrequency (DTMF) tones from breaking dial tone from Communication Manager.

Use the **`status remote-access`** command to view the status of a Remote Access barrier code.

Call Detail Recording (CDR) does not track the use of barrier codes.

Authorization codes with Remote Access

You can administer authorization codes to manage access to your system. You can then use Call Detail Recording to track the use of authorization codes. Use the following guidelines to manage the use of authorization codes.

- Assign authorization codes that:
  - Are random, nonconsecutive, and unpredictable
  - Are the maximum code length that the system allows
  - Are unique to each person who uses an authorization code
  - Have the minimum level of calling permissions that a user requires
- Change codes frequently, at least quarterly.
- Delete codes when the codes are no longer needed.
- Delete codes when a user leaves the company, or changes job assignments.
- Use CDR reports to monitor and analyze the use of the codes.

Alternate Facility Restriction Levels with Remote Access

Consider the use of Alternate Facility Restriction Levels (AFRLs) instead of Facility Restriction Levels (FRLs) after normal business hours to restrict where calls can be made over your facilities. Do not restrict callers from summoning emergency services after normal business hours.

Class of Restriction Remote Access

The COR of an authorization code supersedes the COR of a barrier code.

- Time of Day Routing is controlled by the time-of-day entries in the COR or by the partition.
- Toll Restriction and Analysis is controlled by COR.
- Trunk Access Code (TAC) interacts with toll restriction. You can translate Communication Manager so that users can use ARS to make toll calls, without the need for a TAC.
- The Authorization Code COR overrides the Barrier Code COR, the Barrier Code COR in turn overrides the VDN COR, and the VDN COR in turn overrides the COR of the originator.

For additional steps to secure your system, and to obtain security information on a regular basis, see the *Avaya Toll Fraud and Security Handbook*.

Logoff Notification with Remote Access

Use Logoff Notification when you enable Remote Access for your system, but your users are not using Remote Access actively. Logoff Notification notifies you when you log off the system that Remote Access is enabled.

Logoff Notification alerts you to an unauthorized activation of the Remote Access feature. Logoff Notification is administered by login ID.

Remote Access administration

The following tasks are part of the administration process for the Remote Access feature:

- Enabling Remote Access
- Disabling Remote Access
- Administering authorization codes for Remote Access
- Administering Remote Access for Night Service

Related links

[Enabling Remote Access](#) on page 1168
[Disabling Remote Access](#) on page 1170
[Administering authorization codes for Remote Access](#) on page 1170
[Administering Remote Access for Night Service](#) on page 1172

Screens for administering Remote Access

Screen name	Purpose	Fields
Authorization Code - COR Mapping	Assign pairs of authorization codes and Classes of Restriction (CORs).	• AC • COR
Feature-Related System Parameters	Assign the length of the authorization codes.	Authorization Code Length
Optional Features	Enable authorization codes.	Authorization Codes
Remote Access	Enable Remote Access.	All
	Disable Remote Access	Permanently Disable
Trunk Groups • CO • DID • FX • ISDN-BRI • ISDN-PRI • WATS	Assign Remote Access for Night Service.	• Incoming Destination • Night Services

Enabling Remote Access

Procedure

1. Enter `change remote-access`.
2. In the **Authorization Code Required** field, perform one of the following actions:
   - If you want a user to enter an authorization code to use Remote Access, type `y`.
   - If you do not want a user to enter an authorization code when the user uses Remote Access, type `n`.

The **Calls Used** field is a display-only field that shows the number of calls that are placed with the corresponding barrier code. The system increments this field whenever a barrier code is successfully used to access the Remote Access feature.

3. In the **Barrier Code** field, perform one of the following actions:
   - Type a barrier code.

     The number that you type in the **Barrier Code Length** field determines the number of digits that you type in this field.
   - If the **Barrier Code Length** field is blank, you must type `none` in the first **Barrier Code** field.

     You can assign 10 barrier codes to your system. You cannot assign duplicate barrier codes.
4. In the **Barrier Code Length** field, type the length of the barrier codes that you want to use in your system.

   Valid entries are the numbers 4 through 7. You can also leave this field blank.
5. In the **COR** field, type the COR number that is associated with the barrier code.

   The barrier code defines the call restriction features.
6. In the **COS** field, type the COS number that is associated with the barrier code.

   The barrier code defines access permissions for Call Processing features. Valid entries are the numbers 0 to 15.
7. In the **Disable Following a Security Violation** field, perform one of the following actions:
   - If you want the system to disable the Remote Access feature when the system detects a remote access security violation, type `y`.
   - If you do not want the system to disable the Remote Access feature when the system detects a remote access security violation, type `n`.

   The system displays the **Disable Following a Security Violation** field when the **SVN Authorization Code Violation Notification Enabled** field on the Security-Related System Parameters screen is set to y.
8. In the **Expiration Date** field, type the date that you want the barrier code to expire.

   You must type a date that is greater than the current date. You can also leave the field blank.

   If you assign an expiration date, the system displays a warning message on the System Copyright screen 7 days before the expiration date of the barrier code. If you want to extend the expiration date, change the date in this field.
9. In the **No. of Calls** field, type the number of times that users can use the barrier code for Remote Access.

   Valid entries are the numbers 1 to 9999.
10. In the **Permanently Disable** field, type `n`.

11. In the **Remote Access Dial Tone** field, perform one of the following actions:
    - If you want the system to provide a Remote Access dial tone prompt, type `y`.
    - If you do not want the system to provide a Remote Access dial tone prompt, type `n`.

    Security alert:

    To maintain system security, Avaya recommends that you set this field to n.

    The system displays this field only when the **Authorization Code Required** field is set to y.
12. In the **Remote Access Extension** field, perform one of the following actions:
    - If no barrier codes exist, leave the field blank.
    - If barrier codes exist, type the Remote Access extension.

      The remote access extension is used like a DID extension. Only one DID extension can be assigned as the Remote Access extension. Calls to the Remote Access extension are treated the same as calls on the remote access trunk.
13. In the **TN** field, type the Tenant Partition number.

    Valid entries are the numbers 1 to 100.
14. Select **Enter** to save your changes.

Disabling Remote Access

Procedure

1. Enter `change remote-access`.
2. In the **Permanently Disable?** field, type `n`.
3. Select **Enter** to save your changes.

Administering authorization codes for Remote Access

Before you begin

On the Optional Features screen, ensure that the **Authorization Codes** field is set to y. If the **Authorization Codes** field is set to n, your system does not support authorization codes. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering authorization codes for Remote Access, or to open a service request.

To view the Optional Features screen, enter `display system-parameters customer-options`.

Procedure

1. Administer authorization code Feature-Related System Parameters.
2. Assign authorization codes.

Administering authorization code Feature-Related System Parameters

Procedure

1. Enter `change system-parameters features`.
2. In the **Authorization Codes Enabled** field, perform one of the following actions:
   - If you want the users to use authorization codes, type `y`.
   - If you do not want the users to use authorization codes, type `n`.

   You can administer this field only if the **Authorization Codes** field on the Optional Features screen is set to y.

   Security alert:

   To maintain system security, Avaya recommends that you set the **Authorization Codes Enabled** field to `y`.
3. In the **Authorization Code Length** field, type the length of the authorization codes.

   Authorization codes must be between 4 and 13 digits long.

   The system displays this field only if the **Authorization Codes Enabled** field is set to y.

   Security alert:

   To maintain system security, Avaya recommends that you use the maximum length for the authorization code.
4. In the **Authorization Code Cancellation Symbol** field, perform one of the following actions:
   - If both the main server and the tandem server are the same type of server, type `#`.
   - If an Avaya System 85 or a DIMENSION is involved, type the number `1`.

     A user dials the authorization code cancellation symbol to cancel the 10-second wait period, during which the user can enter an authorization code

   The system displays this field only when the **Authorization Codes Enabled** field is set to y.
5. In the **Attendant Time Out Flag** field, perform one of the following actions:
   - If you want the system to route a call to the attendant if a user does not dial an authorization code within the 10-second wait period, or if a user dials an invalid authorization code, type `y`.
   - If you do not want the system to generate an intercept tone if a user does not dial an authorization code within the 10-second wait period, or if a user dials an invalid authorization code, type `n`.

   The system displays this field only when the **Authorization Codes Enabled** field is set to y.

6. In the **Display Authorization Code** field, perform one of the following actions:
   - If you want the system to display the authorization code as the user dials the authorization code, type `y`.
   - If you do not want the system to display the authorization code as the user dials the authorization code, type `n`.

   This field applies only to digital communication protocol (DCP) telephones. The field does not apply to ISDN-BRI or hybrid sets.

   Security alert:

   To enhance the security of your system, Avaya recommends that you set the **Display Authorization Code** field to n.
7. Select **Enter** to save your changes.

Assigning authorization codes for Remote Access

Procedure

1. Enter `change authorization-code`.

   The **Number of Codes Administered** field is a display-only field. This field contains the number of authorization codes that you administered on the Authorization Code - COR Mapping screen. The system limits the number of authorization codes that you can administer. To determine the number of authorization codes that you can administer, type **display capacity**.
2. In the **AC** field, type the length of the authorization codes.

   Authorization codes must be between 4 and 13 digits long.

   The number of digits that you type in this field must be the number of digits that you assigned to the **Authorization Code Length** field on the Feature-Related System Parameters screen.
3. In the **COR** field, type the Class of Restriction (COR) that the system uses when a user enters the associated authorization code.
4. Select **Enter** to save your changes.

Administering Remote Access for Night Service

Procedure

1. Enter `change trunk-group` *n*, where *n* is the number of the trunk group for which you want to administer Remote Access for Night Service.
2. In the **Incoming Destination** field, type `attd`.

   The system displays the **Incoming Destination** field, when the **Direction** field is set to incoming or two-way.
3. In the **Night Service** field, type the Remote Access extension.

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

End-user procedures for Remote Access

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Accessing the attendant with Remote Access

Procedure

1. Enter the Remote Access extension.
2. Enter the barrier code.
3. Enter the attendant access code.

Considerations for Remote Access

This section provides information about how the Remote Access feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Remote Access under all conditions. The following considerations apply to Remote Access:

- After the baud of a digital-terminal data module (DTDM) is changed from 9600 to 1200, the DTDM cannot be accessed by Remote Access until an internal call is made to the DTDM.

Interactions for Remote Access

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

Abbreviated Dialing

Remote Access Users can access the group-number, system-number, and enhanced-number Abbreviated Dialing lists administered on the Console form.

Authorization Codes

When a Remote Access caller dials the assigned Remote Access extension and connects to the system, the system can request the caller to dial an authorization code in addition to a barrier code. Dial tone between the barrier code and authorization code is optional. Calling privileges

that are associated with the Class of Restriction (COR) that is assigned to the authorization code supersede the calling privileges that are assigned to the barrier code.

Call Detail Recording (CDR)

CDR tracks the use of authorization codes. CDR does not track the use of barrier codes.

Class of Restriction (COR)

COR restrictions do not block access to the Remote Access feature.

Night Service

You can specify the Remote Access extension as the Night Service extension on incoming, non-direct inward dialing (DID) trunk groups.

Chapter 152: Restriction - Controlled

With the Restriction - Controlled feature, a user with console permission can:

- Activate and deactivate specific restrictions for an individual user or an attendant
- Activate and deactivate specific restrictions for all users or attendants who have a specific Class of Restriction (COR)

Detailed description of Restriction - Controlled

With Restriction - Controlled, a user with console permissions can:

- Activate and deactivate specific restrictions for an individual user or an attendant
- Activate and deactivate specific restrictions for all users or attendants who have a specific Class of Restriction (COR)

Use Restriction - Controlled to administer the following restrictions:

Outward

The user cannot place calls to the public network.

Total

The user cannot place or receive calls, with the following exceptions:

- Calls to a remote-access extension
- Terminating-trunk transmission tests
- Emergency Access to Attendant calls

Termination

The user cannot receive any calls. The system:

- Routes incoming calls to the attendant
- Redirects calls to the Call Coverage path
- Uses Restriction - Controlled intercept treatment

Station-to-Station

The user cannot place or receive station-to-station calls.

Restriction - Controlled administration

This section describes the screens that you use to administer the Restriction - Controlled feature.

Screens for administering Restriction - Controlled

Screen name	Purpose	Fields
Feature Access Code (FAC)	Specify the Feature Access Codes (FACs) for Restriction - Controlled.	• User Control Restrict Activation and Deactivation • Group Control Restrict Activation and Deactivation
Feature-Related System Parameters	Specify the type of intercept treatment that the system uses for Restriction - Controlled.	• Controlled Outward Restriction Intercept Treatment • Controlled Termination Restriction (Do Not Disturb) • Controlled Station-to-Station Restriction

End-user procedures for Restriction - Controlled

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Activating Restriction - Controlled

Procedure

1. Dial the Feature Access Code (FAC) with which you can apply Restriction - Controlled to an extension or an attendant group.
2. Dial the number for the type of restriction that you want:
   - for outward
   - for total
   - for termination
   - for station-to-station
3. Perform one of the following actions:
   - If you want to apply Restriction Controlled to an individual extension, dial the extension.
   - If you want to apply Restriction Controlled to all users and attendant who are assigned a certain Class of Restriction (COR), dial the number of the class of restriction (COR).

Considerations for Restriction - Controlled

This section provides information about how the Restriction - Controlled feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Restriction - Controlled under all conditions. The following considerations apply to Restriction - Controlled:

- All telephones with the same COR are affected by a group restriction. When a call is placed, the system checks both the individual and the group restrictions.

Interactions for Restriction - Controlled

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

Call Coverage

The system does not check controlled restrictions for covering users.

Call Forwarding

The system checks the controlled restrictions for the forwarded-to extension, when Call Forwarding All Calls is active.

Class of Restriction (COR)

The system checks the COR when a call is authorized.

Priority Call

If a user activates priority calling before the user dials another extension, the calling user receives intercept tone. The user receives the intercept tone whether you set **Controlled Station to Station Restriction** field on the Feature-Related System Parameters form to y or n.

Uniform Call Distribution (UCD)

The system does not apply Restriction - Controlled to calls that are dialed through the Uniform Dial Plan (UDP).

Chapter 153: Ringing - Abbreviated and Delayed

Use the Ringing - Abbreviated and Delayed feature to assign one of four ring types to each call appearance on a telephone. The ring type that you assign to a call appearance is automatically assigned to each of the bridged call appearances of each call appearance.

Set the **Auto-A/D** field on the Station screen to y, to enable the automatic abbreviated/delayed ringing for a call appearance. The type of ringing for each call depends on the **Rg** field setting. For more information about the fields, see *Avaya Aura® Communication Manager Screen Reference*.

Detailed description of Ringing - Abbreviated and Delayed

The Ringing - Abbreviated and Delayed feature has two categories of ringing:

- Ringing that alerts consistently and does not change:
  - Ringing, in which the lamp flashes and audible ringing occurs
  - Silent ringing, in which the lamp flashes and audible ringing does not occur
- Ringing that transitions from one ringing state to another:
  - Abbreviated ringing, in which ringing continues for the number of cycles that you specify with the automatic abbreviated transition interval or the delayed transition interval, and then changes to silent alerting
  - Delayed ringing, in which visual alerting continues for the number of cycles that you specify with the automatic abbreviated transition interval or the delayed transition interval, and then changes to ringing

When you administer the Station screen of a user, you can assign an abbreviated dial button of that user to another user. The user of the Station screen that you administer must have a telephone with call appearances that have either abbreviated or delayed ringing. When a call alerts at one of those call appearances, the user presses the button. When the user presses the button, the system forces an immediate transition from ringing to silence, or from silence to ringing.

The Ringing - Abbreviated and Delayed feature is most useful in bridging situations in which some users want to:

- Have a call audibly alert as soon as the call arrives
- Be audibly notified if the call is unanswered within a specified number of rings
- Stop the audible alerting if the call is unanswered by the called party, and the user cannot answer the call

You specify the types of ringing on the Station screen of each user in your system. You can assign one of the following ring types to each telephone line button.

- Abbreviated Ring

  A call rings the telephone until the automatic or the manual automatic abbreviated transition or the delayed transition occurs. After the transition, the call silently alerts at the telephone.

- Delayed Ring

  A call silently alerts the telephone until the automatic or the manual abbreviated transition or the delayed transition occurs. After the transition, the call rings at the telephone.

- No Ring

  A call silently alerts the telephone and does not transition.

- Ring

  A call rings at the telephone and does not transition.

When a user presses the abbreviated-ring button on the telephone, the system performs an abbreviated transition or a delayed transition for all calls at the extension. Calls to other extensions that alert at the telephone are unaffected.

Ringing - Abbreviated and Delayed administration

The following tasks are part of the administration process for the Ringing - Abbreviated and Delayed feature:

- Assigning per button ring control to a user
- Assigning an abbreviated ringing button to a user

Related links

Assigning per button ring control to a user on page 1180
Assigning an abbreviated ringing button to a user on page 1181

Preparing to administer Ringing - Abbreviated and Delayed

About this task

Before you can administer the Ringing - Abbreviated and Delayed feature, you must assign the number of rings before a transition.

Procedure

1. Enter `change system-parameters features`.
2. In the **Auto Abbreviated/Delayed Transition Interval (rings)** field, type the number of rings before the system performs an automatic abbreviated transition or delayed transition for a call.

   You can type a number from 1 to 16.
3. Select **Enter** to save your changes.

Screens for administering Ringing - Abbreviated and Delayed

Screen name	Purpose	Fields
Feature-Related System Parameters	Assign the number of rings before the system performs an automatic abbreviated transition or a delayed transition for a call.	Auto Abbreviated/Delayed Transition Interval (rings)
Station	Allow a user to select ringing for call appearances.	• Per Button Ring Control • Auto-A/D • Rg
	Assign an **abrv-ring** button to a user.	Any available button field in the **Feature Buttons** area

Assigning per button ring control to a user

Procedure

1. Enter `change station n`, where *n* is the number of the extension to which you want to assign ring control for a user.
2. Click **Next** until you see the **Per Button Ring Control** field.
3. In the **Per Button Ring Control** field, perform one of the following actions:
   - Type `y` if you:
     - Want users to select ringing individually for each call appearance, bridged call appearance, or analog bridged call appearance on the telephone, and
     - Want to enable the automatic abbreviated and delayed ring transition for each call appearance on the telephone, and
     - Do not want the system to automatically move the line selection to a silently alerting call, unless that call was audibly ringing earlier
   - Type `n` if you want:
     - Calls on call-appr buttons to always ring the telephone, and
     - The value in the **Bridged Call Alerting** field of the Station screen to control whether calls ring on the brdg-appr or the abrdg-appr buttons, and

- The system to move the line selection to a silently alerting call, if no call is audibly ringing the telephone

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

Assigning an abbreviated ringing button to a user

Procedure

1. Enter `change station n`, where *n* is the number of the extension to which you want to assign an abbreviated and delayed feature button for a user.
2. Click **Next** until you see the **Button Assignments** area.
3. Type `abrv-ring` next to the button that you want the user to use to cause a call that rings to transition from ringing to silence, or silence to ringing.

   When you type `abrv-ring` next to the button, the system displays an **Ext:** field.
4. (Optional) In the **Ext:** field, type the extension of the other user to whom you want to assign the abbreviated ringing button.
5. Select **Enter** to save your changes.

Considerations for Ringing - Abbreviated and Delayed

This section provides information about how the Ringing - Abbreviated and Delayed feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Ringing - Abbreviated and Delayed under all conditions. The following considerations apply to Ringing - Abbreviated and Delayed:

- You cannot assign Ringing - Abbreviated and Delayed to an attendant console.
- You can assign the Ringing - Abbreviated and Delayed feature to analog telephones. However, because analog telephones cannot visually alert, a user can unexpectedly answer an incoming call, when the user intends to originate a call.

Interactions for Ringing - Abbreviated and Delayed

This section provides information about how the Ringing - Abbreviated and Delayed feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Ringing - Abbreviated and Delayed in any feature configuration.

Call Coverage

If the number-of-rings interval for coverage is shorter than the automatic transition interval, the system redirects the call to coverage before the system audibly alerts a call appearance that has

delayed ringing. However, the system continues to increment the timer for the automatic transition interval, in case no coverage point is available, and the call continues to alert at the telephone.

When a call is immediately redirected to coverage, the Ringing - Abbreviated and Delayed ringing has no effect on the system processes.

Call Forwarding - Busy/Don’t Answer

When the system forwards a call because no one answers the call in the specified interval, the call stops alerting at the telephone. The Ringing - Abbreviated and Delayed feature does not affect the manner in which the system processes the call. However, the system continues to increment the timer for the automatic transition interval, in case forwarding fails, and the call continues to alert at the telephone.

If the interval for call forward don’t answer is shorter than the interval for automatic transition, the system redirects the call to the forwarded-to extension before the call rings at a telephone that has a ring type of delayed ringing.

Call Vectoring - Expert Agent Selection - Logical Agents

Calls that the system routes to a logical agent use the translations for the Ringing - Abbreviated and Delayed feature of the telephone that the agent uses.

Data Extension Calls

Data Extension calls are unaffected by the ring values. The calls continue to be directed according to the way that you administered bridged call alerting.

Hospitality Features - Do Not Disturb

The Do Not Disturb feature takes precedence over the Ringing - Abbreviated and Delayed feature in blocking ringing to the telephone.

Integrated Services Digital Network (ISDN) - World Class Basic Rate Interface (BRI)

Several of the protocol variations that the World Class BRI feature restrict the messaging that is required for control of a telephone ringer by the Ringing - Abbreviated and Delayed feature. If the protocol variations do not permit the required messaging for the telephone ringer, the system rings the call at the telephone, and does not transition the ring.

Multiappearance Preselection and Preference

If the **Per Button Ring Control** field on the Station screen is set to n, the system automatically selects any call that alerts at a telephone. The call can alert in a manner other than ringing.

If the **Per Button Ring Control** field on the Station screen is set to y, the system automatically selects any call that rings at a telephone.

Off-Premises Station (OPS) and Off-Premises Extension (OPX) lines

You must use a ring type of ring for OPS and OPX lines.

Personal Central Office Line (PCOL) calls

Ring values do not affect the processing of PCOL calls. PCOL calls continue to be directed according to the way that you administer bridged call alerting.

Redirection Notification

If you enable Redirection Notification, telephones receive redirection notification only if the alerting button, or the first call appearance, has an assigned ring value of ring or abrv-ring.

Terminating Extension Group (TEG) calls

Ring values do not affect the processing of TEG calls. TEG calls continue to be directed according to the way that you administer bridged call alerting.

Voice mail systems

Voice mail systems might look for ringing that is applied to a port to trigger call answer. Ring-type translations that are inappropriately set for ports that serve a voice mail system, can result in undesirable operation of the adjunct.

Chapter 154: Security Violation Notification

Use the Security Violation Notification (SVN) feature to notify a designated referral point about a possible security violation. A designated referral point can be an attendant console, a display-equipped telephone, or a telephone without a display for SVN referral calls with announcements.

The system monitors and reports on the following types of security violations:

- Authorization code violations

Communication Manager provides the option to log a major alarm if a security violation occurs involves an Avaya services login ID. Avaya is responsible for retiring the alarm.

Detailed description of Security Violation Notification

To effectively monitor the security of your system, you must know how often both valid and invalid attempts at system entry are normally made. A significant increase in such attempts can mean the system is being compromised.

Note:

Avaya recommends that you print and clear the security violation measurement reports at least once a month. In a busy system, you must print security-violation measurement reports often.

Security violation thresholds and notification

For example, you might determine that during a 40 hour week, the normal condition is for users to submit about 1,000 valid barrier codes and 150 invalid barrier codes. That is, about 3.75 invalid barrier codes submitted per hour.

With this information, you might decide to declare that a security violation occurs during any hour in which eight invalid barrier codes are submitted. If you know that during an 8-hour period, about 30 invalid codes are submitted, you might set the threshold to count a security violation when 40 invalid codes are submitted within eight hours.

You can administer SVN to place a referral call to the location of your choice whenever the established thresholds are reached. All SVN referral calls are priority calls.

Invalid attempts accumulate at different rates for login, authorization-code, remote-access, and station-security code depending on feature usage and the number of users on a server. For this reason, you administer thresholds separately for each type of violation.

SVN sequence of events

The following sequence of events occurs when an SVN is enabled and a detects a security violation:

1. The number of invalid attempts that are permitted in a specified time interval is exceeded.
2. An SVN referral call (with announcements, if assigned) is placed to a designated point, and SVN provides an audit trail that contains information about each attempt to access server that is running Communication Manager.
3. SVN disables a login ID or remote access following the security violation.
4. The login ID or remote access remains disabled until someone with an authorized login ID, with the correct permissions reenables it.

SVN reporting

The system reports information about security violations in the following ways:

- In real time. You can use the **`monitor security-violations`** command to monitor security violations as they may be occurring. Enter this command, and then the type of security violation you want to monitor (logins, remote-access, authorization-codes, or station-security-codes).
- On an immediate basis. When a security violation occurs, the system sends a priority call to a designated referral point (attendant console or telephone). Thus, there is some chance of apprehending the violator during the attempted violation.

  Upon notification, you can request the Security Violations Status Reports, which show details of the last 16 security violations of each type. The Barrier Code and Authorization Code reports, also include the calling party number from which the attempt was made, where available.
- On a historical basis. The number of security violations of each type and other security measurements, are collected and displayed in the Security Violations Summary and Detail reports. These reports show summary information since the counters were reset by the **`clear measurements security-violations`** command or since system initialization. These reports do not show all aspects of the individual security violations.

SVN - halt buttons

You can administer buttons for the notification extension to stop notification calls. However, this might pose a security risk. Do not use these buttons if you do not really need them.

To find out what svn - halt buttons exist in the system, enter `display svn-button-location`.

SVN Referral Call with Announcement

The SVN Referral Call with Announcement option can provide a recorded message with the referral call identifying the type of violation. You can use Call Forwarding, Call Coverage, or Call Vector Time-of-Day Routing to route to an extension or a number off the media server or switch. SVN referral calls with announcements terminate to a point that is either on or off the switch.

Use of other means to route SVN referral calls to alternate destinations are not supported at this time. An attempt to use an alternate method to route SVN referral calls might result in a failure to receive the call or to hear the announcement.

Security violation responses

When a security violation occurs, you can disable the login ID or the remote access privileges of the user who commits the violation.

Disabling a login ID upon SVN

Procedure

1. Log in to Communication Manager with a login ID that has the correct permissions.
2. Enter `disable login n`, where *n* is the login ID of the user.

Enabling a login ID after a SVN

Procedure

1. Log in to Communication Manager with a login ID that has the correct permissions.
2. Enter `enable login n`, where *n* is the login ID of the user.

Enabling remote access after a SVN

Procedure

1. Log in to Communication Manager with a login ID that has the correct permissions.
2. Enter `enable remote-access`.

Disabling remote access upon SVN

Procedure

1. Log in to Communication Manager with a login ID that has the correct permissions.
2. Enter `disable remote-access`.

Security Violation Notification administration

The following task is part of the administration process for the Security Violation Notification (SVN) feature:

- Setting up Security Violation Notification

Related links

Setting up Security Violation Notification on page 1187

Screens for administering Security Violation Notification

Screen name	Purpose	Fields
Login Administration	Set up security violation notification.	Disable Following A Security Violation
Security-Related-System Parameters	Set up security violation notification.	• SVN Login Violation Notification • Originating Extension • Referral Destination • Login Threshold • Time Interval
Remote Access	Set up security violation notification.	Disable Following A Security Violation
Station	Set up security button assignments.	Any available button field in the **Button Assignments** area

Setting up Security Violation Notification

Procedure

1. Enter `change system-parameters security`.
2. In the **SVN Login Violation Notification Enabled** field, type `y`.

   This action sets Security Violation Notification login violation notification.

   Note:

   If you are not using Security Violation Notification for logins, type `n` in the **SVN Login Violation Notification Enabled** field and go to Step 11.
3. In the **Originating Extension** field, type `3040`.

   This becomes the telephone extension for the purpose of originating and identifying SVN referral calls for login security violations.
4. In the **Referral Destination** field, type `attd` to send all calls to the attendant.

   This is the extension of the telephone that receives the referral call when a security violation occurs.

5. In the **Login Threshold** field, type `3`.

   This is the minimum number of login attempts that are permitted before a referral call is made. More than 3 attempts causes a security violation notification.

6. In the **Time Interval** field, type `0:03`.

   This the time interval in which the threshold, or number of violations, must occur.

7. Select **Enter** to save your changes.
8. (Optional) Enter `change login nnnn`, where *nnnn* is your login ID.
9. (Optional) In the **Disable Following A Security Violation** field, type `y`.

   This disables a login following detection of a login security violation for the login you are administering.

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

    Note:

    If you are not using Remote Access, go to Step 14.

11. (Optional) Enter `change remote-access`.
12. (Optional) In the **Disable Following A Security Violation** field, type `y`.

    This disables remote access following detection of a remote access security violation.

13. (Optional) Select **Enter** to save your changes.
14. Enter `change station n`, where *n* is the station that you want to assign to the notification halt button.
15. Click **Next** until you see the **Button Assignments** area.
16. In the **Button Assignments** area, type one of the following values:

    - `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 four security violations causes 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.

17. Select **Enter** to save your changes.

Reports for Security Violation Notification

The following reports provide information about the Security Violation Notification feature:

- The Security Violations Status Report shows details of the last sixteen violations of each type. The Barrier Code and Authorization Code reports also include the calling party number from which the attempt was made, if that number is available.

For detailed information on these reports and the associated commands, see *Avaya Aura® Communication Manager Reports*.

Considerations for Security Violation Notification

This section provides information about how the Security Violation Notification feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Security Violation Notification under all conditions. The following considerations apply to Security Violation Notification:

- You may administer only one referral destination per system for each type of violation.
- Use caution when you administer bridged appearances for stations that are used as SVN referral destinations. SVN referral calls terminating to bridged appearances must be accompanied by an announcement message or must route to bridge appearances equipped with a display module. SVN referral calls that do not have an announcement and terminate to a bridged appearance that does not have a display to provide an indication of the nature of the call.
- An authorization code violation with remote access generates two SVNs. One displays authorization code violation and the second SVN displays barrier code violation, even though the correct barrier code was input. These two displays help you determine that the violation took place in the context of a remote access attempt, and not an attempt to place an outgoing call to an ARS trunk.

Interactions for Security Violation Notification

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

Call Coverage, Call Forwarding, and Call Pickup

These features are supported for SVN only if you use recorded announcements.

Centralized Attendant Services (CAS)

CAS attendants cannot receive SNV referral calls from branch locations.

Distributed Communications System (DCS)

SVN does not support referral calls across a DCS network.

Chapter 155: Selection of DID Numbers to Guest Rooms

Custom Selection of VIP DID Numbers

Using Custom Selection of VIP DID numbers, you can select the DID number assigned to a room when a guest checks in. It also provides buttons on display sets with which you can check in a VIP (the vip-chkin button), view and change XDID and XDIDVIP numbers (the did-view button), and dissociate XDID and XDIDVIP numbers outside of the normal guest check-out procedure (the did-remove button).

Ensure that the following fields are administered to use Custom Selection of VIP DID Numbers:

- the **Basic Hospitality** field on the Feature Related System Parameters Customer Options screen is y
- the **Custom Selection of VIP DID Numbers** field on the Feature Related System Parameters Hospitality screen is y
- the **Automatic Selection of DID Numbers** field on the Feature Related System Parameters Hospitality screen is y

You also need to set up a number of stations as xdidvip (enter `xdidvip` in the **Type** field on the Station screen).

When you use the vip-chkin button on a display telephone to check in a guest, you receive prompts to enter the room extension number and the VIP DID number. Use the did-view button to change a DID number that is automatically assigned by Communication Manager (XDID), or one you select yourself (XDIDVIP).

Use **`list station`** to see which VIP DID numbers are administered. Check the **hunt-to station** field to see if an XDIDVIP number is available or is assigned to a guest room.

Automatic Selection of DID Numbers to Guest Rooms

You can activate Automatic Selection of DID Numbers to Guest Rooms to assign telephone numbers to guests upon check in. With this feature, telephones can have direct dial access to guest rooms. Communication Manager automatically chooses a number from a rotating list of available DID numbers to be assigned to a guest's room. This provides a measure of privacy to your guests because providing the telephone number does not give away the room number.

Callers would use a 7- to 10-digit number from outside of the hotel. For calls from inside the hotel, callers would use either the room/extension number or the 2- to 5-digit DID number.

For example, when a check-in is done from Communication Manager (through the check-in button on the console) or remotely via a Property Management System (PMS) system, Communication Manager assigns a DID number to the checked-in room from a list that is assigned at the server. All calls made to the DID number are directed to the room as if the room was called directly.

Interactions for Automatic Selection of DID Numbers to Guest Rooms

This section provides information about how the Automatic Selection of DID Numbers to Guest Rooms feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Automatic Selection of DID Numbers to Guest Rooms in any feature configuration.

Coverage

XDID ports perform hunt-to before coverage. After hunting, coverage criteria for these calls is based upon the DID, but the coverage points are based upon the hunted-to telephone (room).

Class of Service

Do not assign a Class of Service (COS) with Client Room enabled for the XDID station types.

Chapter 156: Send original calling number to the service link for H.323 Avaya one-X® Communicator

Users who have Avaya one-X® Communicator in the Telecommuter mode on the personal computers have Other Phone configured as the mobile number. When the user receives an incoming call, the number that the mobile displays is the extension number and not the original caller ID.

To allow the user to see the original caller ID instead of the extension, set the **Caller ID for Service Link Call to H.323 1xC** field on the Trunk Group screen to `original-calling-number`. Before sending the call to the service link, Communication Manager changes the calling party number to the original calling party number.

The default value of the **Caller ID for Service Link Call to H.323 1xC** field is station-extension. Communication Manager does not change the calling party number when the value is station-extension.

Caller ID for Service Link Call to H.323 1xC is the outgoing service link trunk group field.

Screen for administering Send original calling number to the service link for H.323 Avaya one-X® Communicator

Screen name	Purpose	Field
Trunk Group	Enable the Send original calling number to the service link for H.323 Avaya one-X® Communicator feature.	Caller ID for Service Link Call to H.323 1xC

Limitations of Send original calling number to the service link for H.323 Avaya one-X® Communicator

Calling Party Number Restrictions

Calling party number restrictions applies to the original calling party number.

If the original calling party number is external, Communication Manager passes the number as it is with the value administered in the **Send Calling Number** field. If the original calling party number is internal, Communication Manager passes the number according to the station administration and the value administered in the **Send Calling Number** field.

Chapter 157: Send-nn Feature Calling

Activating the send-nn button allows the user to replace their real caller ID with a different identity for outgoing calls. The user can configure multiple send-nn buttons, so that the user can have the multiple changed caller IDs instead of their actual caller ID. The send-nn button functionality is supported for SIP and H.323 endpoints.

Detailed description of send-nn calling

Use the **Send-nn** button to obscure the original identity of the calling party. Instead, the calling party can configure an alternative identity to display to the destination party. For example, consider a calling party with the extension number 556677. If a calling party wants to mask their presented identity from the receiving party, they enable the send-nn button with an alternative identity (112233) configured. Consequently, when initiating an outgoing call, their identity shows as 112233 to the receiving party.

Communication Manager provides two variations for the **Send-nn** button:

- Permanent (p) Variant: When you configure the send-nn button with the p variant for a particular station, all calls originating from that station display a changed identity configured within Communication Manager whenever they connect with any destination party. You can establish multiple **Send-nn** buttons using the p variant. However, it is important to note that only one **Send-nn** button can be active at any time. If you activate a new **Send-nn** button to exhibit a different identity, the previously activated **Send-nn** button is deactivated.

  To activate the **Send-nn (p)** button on the endpoint, press the **Send-nn (p)** button once.

  When you press a new **Send-nn (p)** button, the new button is active, and any previously activated **Send-nn (p)** button is deactivated.

- Transient (t) Variant: When you press the **Send-nn (t)** button, the **Send-nn (t)** feature becomes active for that particular call, and you are prompted to enter the extension of the destination party to initiate the call as soon as the **Send-nn (t)** button is pressed. After pressing the **Send-nn (t)** button, the green light on the station illuminates for two seconds. This indicates that the **Send-nn (t)** feature is activated specifically for the current call.

  The extension configured at the **Send-nn (t)** button is the changed caller identity.

In addition, it is possible to configure multiple caller IDs for a single station by adding **Send-nn** buttons specific to that station. The extensions configured behind these **Send-nn** buttons must be

unique, regardless of the variant chosen. The **Send-nn** button supports the following stations or set types:

- H.323
- J129
- J179
- J179CC
- J169
- J169CC
- AvyaSIP (J139, J159, and J189)
- AvyaSIPCC (J189CC)

Note:

When a station has an active **Send-nn (p)** button configured with extension 112233, if you press the **Send-nn (t)** button with extension 223344, the specific call made utilizes the extension 223344 as its identity presented to the destination party.

The changed identity number that you intend to showcase to the destination party must adhere to the dial-plan regulations outlined in the Communication Manager. It can be an extension number associated with a station, a hunt group, or a Vector Directory Number (VDN).

Send-nn Feature Calling administration

The following tasks are part of the administration process for the Send-nn Feature Calling:

- Adding a Send-nn button to a SIP phone

Screens for administering Send-nn Calling

Screen name	Purpose	Fields
Station	Assign a **Send-nn** button to a station.	Any available button field in the **Button Assignments** area.

Adding a send-nn button to a phone

Procedure

1. Type `add station n`, where *n* is the extension.

   The **Type** field on the station screen should be one of the specified types that support this feature.

2. On the Station screen, click **Next** until you see the **Button Assignments** field.
3. In the **Button Assignments** field, type `Send-nn` in any of the empty fields to create a **Send-nn** button.

4. After adding the **Send-nn** button, the station page displays the **Ext** and **Md** fields.
5. In the **Ext** field, type the extension of a station, or a hunt group, or a Vector Directory Number (VDN).

   This Extension is used as a changed identity of a user when the user makes any outgoing call from the station.
6. In the **Md** field, type one of the following variants:
   - **p** Variant
   - **t** Variant

   For more information about the type of variant, see Detailed description of send-nn calling on page 1195.
7. Press **Enter** to save changes.

Note:

You must specify the extension for the **Send-nn** button, and this extension must adhere to the dial plan rules configured in Communication Manager.

To add a **Send-nn** button to H.323 stations using the System Access Terminal (SAT) terminal, you enable the **(SA8967) - Mask CLI and Station Name for QSIG/ISDN Calls?** field on the system-parameters special-applications form. This enables you to configure the send-nn button for H.323 stations.

Use System Manager interface for configuring the Send-nn button for SIP stations. This process is independent of the **(SA8967) - Mask CLI and Station Name for QSIG/ISDN Calls?** field.

End user procedures for Send-nn feature calling

End users must perform procedures to use certain features. They can activate or deactivate certain system features and capabilities and modify or customize some aspects of administering certain features and capabilities.

To activate the **Send-nn (p)** button on the endpoint, press the **Send-nn (p)** button once.

When you press the **Send-nn (t)** button, the **Send-nn (t)** feature becomes active. The user are prompted to enter the extension of the destination party to initiate the call. After pressing the **Send-nn (t)** button, the green light on the station illuminates for a duration of 2 seconds. This indicates that the **Send-nn (t)** feature is activated specifically for the current outgoing call.

Activating the Send-nn feature Calling before placing a call

Procedure

1. Press a **Send-nn (p)** feature button and dial an extension.

Whenever the **Send-nn (p)** button is pressed on a station, all calls initiated from the station shows a changed identity configured within Communication Manager whenever they connect with any destination party.

2. Press the **Send-nn (t)** button, and the user is prompted to enter the extension of destination.

Deactivating Send-nn (p) button

About this task

You can use this procedure to deactivate the **send-nn (p)** button.

Procedure

1. Press the currently active **Send-nn (p)** button.
2. Press a new **Send-nn (p)** button.

   When you press a new **Send-nn (p)** button, the new button becomes active, and any previously activated **Send-nn (p)** button is deactivated.

Interactions for Send-nn feature calling

This section provides information about how the **Send-nn** feature calling interacts with other features on Communication Manager. Use this information to ensure that you receive the maximum benefits of the Send-nn feature calling in any feature configuration.

Call Coverage

Communication Manager directs a call to coverage when the user activates the **Go to Cover** option for the call. When the call is redirected to coverage, the extension number configured behind the activated **Send-nn** button becomes the calling party number rather than the original extension number.

Call Forwarding All Calls

Communication Manager forwards send-nn feature calls, excluding callback calls. During call forwarding, the calling party number reflects the extension number configured behind the activated **Send-nn** button rather than the original extension number.

Emergency Call

If the emergency application sequencer is not enabled on System Manager for a station, and the station presses the **Emergency** button to make an emergency call while the **Send-nn (p)** button is activated, the Send-nn feature calling is unavailable for that station. The Public Safety Answering Point (PSAP) station will see the original caller IDs rather than the alternative ID configured behind the activated **Send-nn (p)** button because Communication Manager treats such calls as trunk-originated calls.

However, if the emergency application sequencer is enabled on System Manager for this station, the PSAP station will see the alternative ID configured behind the activated **Send-nn (p)** button. Here Communication Manager treats these calls as station-originated calls.

Note:

The Send-nn feature calling is available only when Communication Manager interprets the call as station-originated based on the configuration done in System Manager.

Limitations of Send-nn Calling

The Send-nn calling button feature has limitations where each extension number configured for the send-nn button must be unique for a station.

Chapter 158: Separation of Bearer and Signaling

Use the Separation of Bearer and Signaling feature to reduce the costs of private leased lines. The Separation of Bearer and Signaling (SBS) feature provides a feature set similar to Distributed Communications Service Plus (DCS+). The SBS feature uses the Public Switched Telephone Network (PSTN) for bearer (voice) element, and QSIG private network signaling over a low-cost IP Network for the signaling element of calls. SBS is available only with Communication Manager.

Detailed description of Separation of Bearer and Signaling

SBS provides a low-cost, virtual private network (VPN) over IP trunks with the high voice quality that is expected of the PSTN. By using SBS, you can save on the costs of private leased lines.

The Separation of Bearer and Signaling (SBS) feature provides a Distributed Communications Service Plus (DCS+)-like feature set using the Public Switched Telephone Network (PSTN) for the bearer (voice) element, and QSIG private network signaling over a low-cost IP Network for the signaling element of calls.With SBS Distributed Communication System Plus (DCS+), you can replace an expensive VPN service if you need Dial Plan Expansion (DPE) functionality. Therefore, you can get enhanced signaling without private leased lines. DCS does not work with 6-digit or 7-digit dial plans. Although QSIG works with 6-digit or 7-digit dial plans, QSIG does not work over VPNs. These VPNs include SDN from AT&T or V-Net from MCI.

SBS also provides a transport mechanism for application data, and other enhanced functionality in locations where ISDN trunking is unavailable or expensive.

The SBS feature supports:

- QSIG private network signaling over a low-cost, IP-based network
- Voice calls, or bearer traffic, over the PSTN
- Correct association between QSIG feature signaling information and each voice call.

You must always use Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), or Uniform Dial Plan (UDP) to originate an SBS call. You cannot use a Trunk Access Code (TAC) or a Dial Access Code to originate an SBS call.

Note:

This SBS feature is strictly a proprietary Communication Manager implementation and does not operate with non-Communication Manager systems. There is no known industry standard that supports Separated Bearer and Signaling calls.

When a user dials a call that is routed to an SBS trunk, two different and separate calls originate. One call carries the signaling portion of the call and the other carries the bearer portion of the call. The following is a high level description of a point to point SBS call.

Call originated

- A signaling call is setup between the SBS Originating Node and the SBS Terminating Node (SETUP and Call PROCEEDING messages).
- An initial SETUP message is sent which has the final destination extension number as the called party.

Complete Number constructed

- The SBS Terminating Node selects a new extension type, SBS Extension, to use for the duration of the call setup. This new extension type indicates that the call was received on an SBS trunk group.
- The SBS Terminating Node, using the public unknown-numbering table, constructs a Complete Number (area/city/extension) for the SBS extension.
- The SBS Terminating Node then adds its country code to the Complete Number and sends this entire number (country code/area/city/extension) to the SBS Originating Node (INFO message).
- With this new number, the SBS Originating Node can establish the bearer call to the SBS Terminating Node.

Complete Number Initiated to SBS Terminating Node

- The SBS Originating Node receives the Complete Number from the SBS Terminating Node and compares the country code in the Complete Number to its own country code.
- If the country codes match, the SBS Originating Node discards the country code.

  or

  If the country codes do not match, the SBS Originating Node adds its International Access Code to the Complete Number.
- The SBS Originating Node uses Automatic Route Selection (ARS) to initiate a call to the SBS Terminating Node using the Complete Number. ARS is always used to initiate the bearer call. ARS uses normal call routing (ARS analysis to pattern/preference) to complete the call. Through the use of digit conversion, for example, the call can be routed using AAR and a private network.

Call completed

- The SBS Terminating Node receives the bearer call to the SBS Extension.
- The SBS Terminating Node determines which SBS signaling call is currently using this particular SBS Extension. The SBS Terminating Node provides a unique ID over the signaling call (INFO message) to the SBS Originating Node.

- The SBS Originating Node passes the unique ID back to the SBS Terminating Node, through DTMF digits over the bearer call.
- The SBS Terminating Node uses the DTMF unique ID to verify that the bearer call is the correct call to associate with the signaling call.
- Once the SBS Terminating Node has associated the signaling and bearer call it completes the call to the called party and returns an ALERTING message to the SBS Originating Node on the SBS signaling call.

Signaling for the SBS signaling call is the same as existing H.323 trunks using QSIG signaling with two exceptions. First, the SETUP and CALL PROCEEDING messages will contain Null Caps. Second, at least two INFO messages will be sent from the SBS Terminating Node to the SBS Originating Node. The INFO messages indicate the number to route the SBS bearer call to, and then the unique ID to signal on the SBS bearer call. These INFO messages are sent after the CALL PROCEEDING, and before ALERTING. They are encoded in a standard fashion, containing a Called Party Number - Information Element (IE).

Typical SBS call connection examples

Four typical call connections are presented here.

- Point to Point call represents an SBS call between two Communication Manager systems. See the figure on page 1202.
- Tandem SBS trunk call represents an SBS call between two Communication Manager systems (A to C) with an intervening Communication Manager system in between. The SBS signaling link tandems through the intervening (B) node. The SBS bearer call is direct from node A to node C. See the figure on page 1203.
- An SBS trunk interworked to a non-SBS trunk represents a call between two Communication Manager systems (A to C) with SBS functionality available only between nodes A and B. This call is interworked from SBS to a non-SBS QSIG trunk group at node B. See the figure on page 1203.
- A non-SBS trunk interworked to an SBS trunk represents a call between two Communication Manager systems (A to C) with SBS functionality only available between nodes B and C. This call is interworked from non-SBS QSIG trunk group to SBS at node B. See the figure on page 1204.

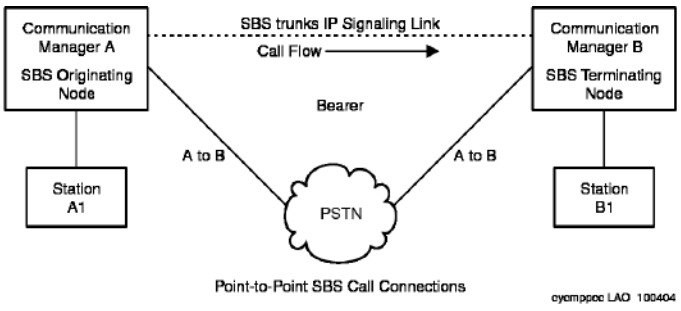


Figure 27: Point to Point SBS Call Connections

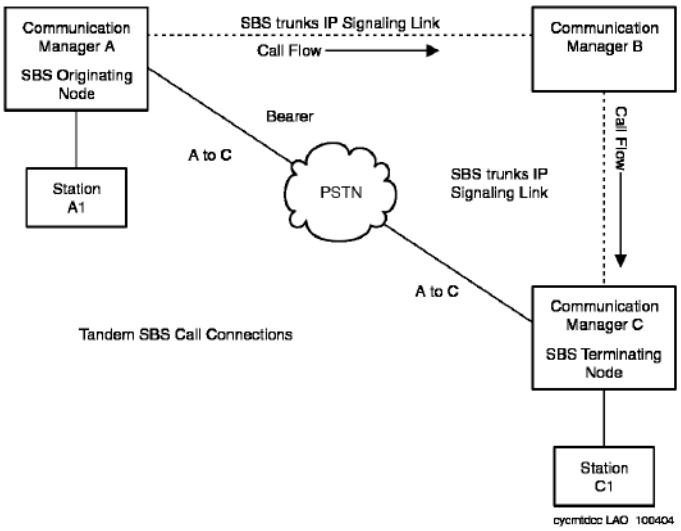


Figure 28: Tandem SBS Call Connections

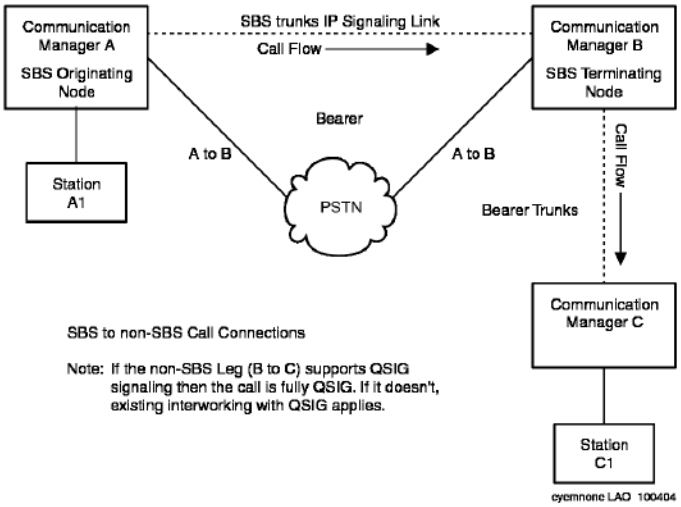


Figure 29: SBS to non-SBS QSIG Call Connections

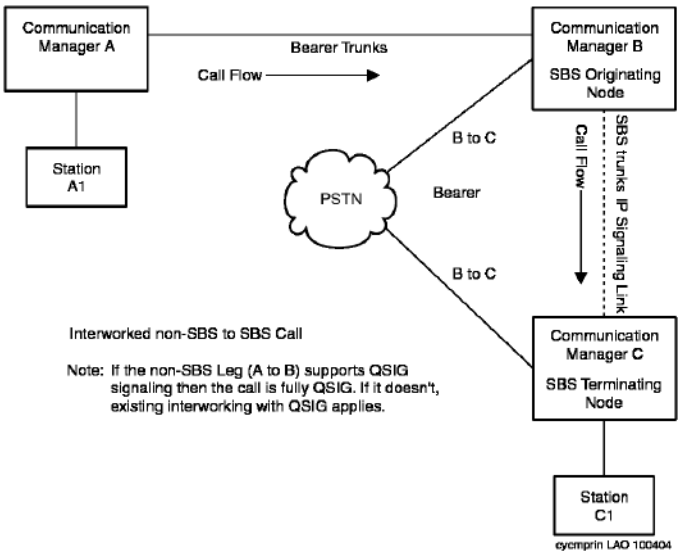


Figure 30: PRI Non-SBS to SBS Call Connections

Typical SBS call setup

The following is a step-by-step description of a typical call.

1. An originating node user goes off hook and dials a terminating node user. The user can dial whatever number of digits are required to reach the terminating user. The originating call may be routed using Uniform Dial Plan (UDP), Automatic Route Selection (ARS), Automatic Alternate Routing (AAR), or a combination of these steering mechanisms.

   Note:

   The call might first route over a non-SBS trunk to an SBS Interworking Node that then routes the call to an SBS trunk. In this case, the SBS Interworking Node, not the originating Node, serves as the SBS Originating Node for this call.

2. Whichever routing mechanism is invoked (UDP/ARS/AAR), the call eventually routes to an H.323 IP trunk group. The call is translated to use QSIG signaling and specified in administration as an SBS trunk group with an SBS signaling group. The QSIG and SBS signaling group identification is the signaling portion of the call. This signaling portion is active for the duration of the call. A translation field identifies the SBS trunk group as reserved for SBS use. The signaling group associated with the SBS trunk group also has specific SBS translation. Apart from these fields, the SBS trunk group and signaling group are translated as a standard IP trunk group with standard QSIG signaling.
3. The SBS Terminating Node receives the signaling call. The SBS Terminating Node knows the call is an SBS call because it arrives on an SBS trunk group. The SBS Terminating Node determines that the called party in the signaling call SETUP message routes to a local extension or a non-SBS trunk. However, the Terminating Node temporarily refrains from terminating the call. Instead, the SBS Terminating Node allocates an SBS Extension to use for the duration of call setup. SBS Extension is a new type of Administered Without Hardware (AWOH) extension that is administered at all nodes that terminate SBS calls.

4. The SBS Terminating Node checks the isdn public/unknown numbering table. Upon finding a match for the SBS Extension, the SBS Terminating Node maps the number to a national (public network) Complete Number, including area/city code if applicable. The SBS Terminating Node also determines the local Country Code from the Feature Related System Parameters screen and adds it to the number created from the ISDN Numbering-Public/Unknown screen. The resulting number includes `Country Code/Area/City/SBS` Extension.
5. The SBS Terminating Node then sends the Complete Number to the SBS Originating Node on the SBS Signaling call. This is the number that the SBS Originating Node uses to route the bearer call.
6. The SBS Originating Node receives the Complete Number. The SBS Originating Node compares the Country Code received to the Country Code that the SBS Originating Node is located in. If the Country Codes are the same, the SBS Originating Node deletes the Country Code from the received number. If the Country Codes are different, the SBS Originating Node adds its SBS International Access Code (from the Feature Related System Parameters screen) to the received number.
7. The SBS Originating Node uses ARS to route on the Complete Number, which may have been modified. The Origination Node then initiates the SBS bearer call to the routed-to bearer trunk.
8. The SBS Originating Node associates the signaling and bearer calls internally.
9. The bearer call arrives at the SBS Terminating Node. The SBS Terminating Node determines that the call is for an SBS Extension and immediately answers the call.
10. The SBS Terminating Node then sends a message to the SBS Originating Node on the signaling call that contains a unique three digit ID. This ID is created by the SBS Terminating Node from the internal call identification. This unique ID is reserved for the duration of the call. The SBS Terminating Node uses this unique ID to determine which bearer call is associated with the SBS signaling call in the event of multiple simultaneous calls to the SBS extension at the SBS Terminating Node. Examples of multiple simultaneous calls to the SBS extension include misdirected PSTN calls, telemarketing calls, and so on
11. The SBS Originating Node then sends the unique ID through DTMF tones, on the bearer call, towards the SBS Terminating Node. The originating user does not hear the DTMF tones.
12. After receiving the unique ID, the SBS Terminating Node associates the proper bearer and signaling calls. The SBS Terminating Node completes the call to the original destination (local extension or non-SBS trunk).
13. The SBS Terminating Node releases the SBS Extension.
14. When the called party is ringing, the SBS Terminating Node sends an ALERTING message to the SBS Originating node on the SBS signaling call.
15. When the called party answers, the SBS Terminating Node sends a CONNECT message to the SBS Originating Node on the SBS signaling call.

16. When either the calling party at the originating node or the called party at the terminating node disconnects the call, both, the bearer and the signaling, calls become inactive.

Tandem SBS calls

Separation of bearer and signaling calls can be tandemed through Communication Manager systems. Either the SBS signaling call or the SBS bearer call can tandem.

When SBS calls tandem through a intervening system you cannot use status commands to determine what bearer call is associated with what signaling call. SBS signaling and bearer calls cannot be associated at tandem nodes.

Tandem SBS bearer call

While the SBS feature is intended to use the Public Switched Telephone Network (PSTN) for transport of the bearer call there is nothing to preclude the use of private point to point (Tie Trunk) facilities to establish the bearer call. The SBS bearer call may also use traditional H.323 IP trunks. When IP trunks are used for transport of the SBS bearer call, appropriate user expectations as to voice quality need to be set.

When private point to point facilities are used to transport the SBS bearer call, all feature transparency and name information is obtained from the associated SBS signaling call. This is true even if the bearer call is transported on facilities capable of providing feature transparency (PRI).

You must administer appropriate steering of extension numbers at intervening nodes to ensure proper routing of tandem bearer calls.

Tandem SBS signaling call

SBS signaling calls can tandem through intervening nodes but those nodes must be Communication Manager systems, equipped with release 1.3 or later. Unlike SBS bearer calls, tandem SBS signaling calls must be carried on SBS trunks for all segments of the call. For more information, see Typical SBS call connection examples.

You must administer appropriate steering of extension numbers at intervening nodes to insure proper routing of tandem bearer calls.

Related links

Typical SBS call connection examples on page 1202

Interworked SBS calls

The SBS Interworking Node is the switch where either:

- an incoming SBS trunk call is routed to a non-SBS trunk (Figure 29: SBS to non-SBS QSIG Call Connections on page 1203),

  or

- an incoming non-SBS trunk call is routed to an SBS trunk (Figure 30: PRI Non-SBS to SBS Call Connections on page 1204).

The SBS Interworking Node is either the SBS Originating Node or the SBS Terminating Node.

- The SBS Interworking Node is the SBS Originating Node when a non-SBS trunk is interworked to an SBS trunk.
- The SBS Interworking Node will be the SBS Terminating Node when an SBS trunk is interworked to a non-SBS trunk.

Feature interworking on SBS calls is supported only to the degree that Communication Manager currently interworks public/private protocols to/from QSIG signaling.

Separation of Bearer and Signaling administration

The following tasks are part of the administration process for the Separation of Bearer and Signaling feature:

- Administering Country Code and International Access Code for SBS
- Administering routing for SBS
- SBS extension administration
- SBS extension mapping

Related links

Administering Country Code and International Access Code for SBS on page 1209
SBS trunks and trunk group administration on page 1210
Administering routing for SBS on page 1212
SBS extension administration on page 1213
SBS extension mapping on page 1214
Verifying SBS system capacities on page 1215

Preparing to administer Separation of Bearer and Signaling

About this task

- Verify that the system is running Communication Manager Release 1.3 or later. Release 1.3 or later is required on all nodes that participate in SBS calls. The nodes can be originating, tandem, and terminating.

1. Enter `display system-parameters customer-options`.
2. Scroll through the Optional Features screens to find the **Maximum Administered IP Trunks** field.

   This field must be greater than 1 and include enough trunks for SBS trunk group use.
3. Scroll through the screens to find the **IP Trunks** field.
4. Set the **IP Trunks** field to `y`.
5. Scroll through the screens to find the QSIG Optional Features screen.

6. Set the **Basic Call Setup** field to `y`.
7. Set the **Basic Supplementary Services** field to `y`.
8. Select **Enter** to save your changes.

Note:

Other QSIG options might need to be activated, depending on your feature functionality requirements.

- Verify port and SBS trunk capacities.
  1. SBS Extensions count against the pool of available ports in the same manner as Administered Without Hardware (AWOH) extensions.
  2. Consider whether SBS trunks that you add to an existing system increase traffic on the PSTN trunks. SBS trunk group members count against the pool of available IP trunks. SBS bearer calls usually use the same trunks as normal local and/or toll PSTN calls. For implementation of the SBS feature, you might have to increase the quantity of trunks to the PSTN.

Screens for administering Separation of Bearer and Signaling

Screen name	Purpose	Fields
Dial Plan Analysis	Define the dial plan for SBS calls on the local system.	All
Feature-Related System Parameters	Specify a valid country code for the SBS signaling trunk groups.	Local Country Code
	Specify the access code that the private switched telephone network (PSTN) requires to route calls out of the country.	International Access Code
ISDN Numbering - Public/ Unknown	Specify information for call processing to create a complete number for the SBS extension when this system is the SBS Terminating Node in an SBS call.	All
Route Pattern	Set the **TSC** field to `y` on the route pattern that SBS signaling calls are directed to.	TSC
Signaling Group	Enable SBS for a signaling group.	Group Type Max number of NCA TSC SBS Trunk Group for NCA TSC Trunk Group for Channel Selection Supplementary Service Protocol Near-end /Far-end Listen Ports

Table continues…

Screen name	Purpose	Fields
Station	Specify the SBS extension.	SBS Extension Type Port
Stations	List assigned SBS extensions	Ext Type
System Capacity	Verify trunk and station maximums for the system.	Trunk Ports IP Trunks Station and Trunk Ports Extensions Stations Records Stations without Ports Station and Trunk Ports
Trunk Group	Enable SBS for a trunk group; add members to the SBS trunk group.	Group Type Carrier Medium Carrier Medium Supplementary Service Protocol SBS NCA-TSC Trunk Member Send Name Send Calling Number Send Connected Number (add members) All

Administering Country Code and International Access Code for SBS

About this task

Administer the Local Country Code and International Access Code at both the SBS Originating and SBS Terminating Nodes using the Feature-Related System Parameters screen.

Procedure

1. Enter `change system-parameters features`.
2. Click **Next** until you see the **International Calling Routing Parameters** fields.
3. In the **Local Country Code** field, enter the three-digit country code for this node.

In the United States this field is populated with 1.

4. In the **International Access Code** field, enter the access code required by the Public Switched Telephone Network (PSTN) to route calls out of the country.
5. Select **Enter** to save your changes.

SBS trunks and trunk group administration

You must administer the H.323 IP trunks, equipped with QSIG signaling, between nodes. These trunks are the signaling portion of SBS calls and are specifically translated as SBS trunks in their trunk group and signaling group administration forms. The number of SBS trunk group members must be engineered for the expected SBS traffic volume.

You must administer the trunks to the local PSTN from each node. These trunks do not have any unique SBS related administration.

Note:

While these trunks are intended to be circuit switched PSTN trunks, there is nothing in the SBS feature operation that precludes the use of other trunks. For example, a second choice for bearer calls may be IP trunks. Voice quality might be affected if you use trunks other than PSTN quality circuit switched trunks.

SBS trunk groups are added in three steps. First, create the trunk group and populate the first two administration screens. Second, create the SBS signaling group. Third, add the trunk members to the SBS trunk group. All of these tasks are performed in a SAT session.

Creating the SBS trunk group

Procedure

1. Enter `add trunk-group n`, where *n* is the number of the trunk group.
2. Click **Next** until you see the **Trunk Parameters** section.
3. Set the **Group Type** field to `ISDN`.
4. Set the **Carrier Medium** field to `H.323`.
5. Set the **Dial Access** field to `n`.
6. The **Supplementary Service Protocol** is always set to b.
7. Click **Next** until you see the **Trunk Features** section.
8. Set the **SBS** field to `y` (default is n).

Note:

The **SBS** field can only be set to y if all the following are true:

- **Carrier Medium** field is set to `H.323`,
- **Dial Access** field is set `n`,
- **Supplementary Services Protocol** field is set to `b`, and

- **Local Country Code** and **International Access Code** fields are administered on the Features Related System Parameters screen. The **Send Name, Send Calling Number** and **Send Connected Number** fields must be set to `y` for the SBS trunk group to enable these capabilities on SBS calls.

9. Set the **NCA-TSC Trunk Member** field to one member of the SBS trunk group.
10. Set the **Send Name** field to `y`.
11. Set the **Send Calling Number** to `y`.
12. Set the **Send Connected Number** to `y`.
13. Select **Enter** to save your changes.

Creating a signaling group for SBS

Procedure

1. Enter `add signaling-group` *n*, where *n* is the signaling group number.
2. Make sure the **Group Type** field is set to H.323
3. Set the **Max number of NCA TSC** field to a number greater than zero.

   Non Call Associated Temporary Signaling Connections (NCA TSC) are used to establish connections and pass messages for features like Message Waiting Indication (MWI) activation and deactivation. QSIG protocol establishes and releases the NCA TSC for each MWI session. When a TSC is established between two Communication Manager systems it sends the message it was established for. The TSC then stays up until there have been a few minutes of inactivity. Depending on traffic, this TSC can be used for multiple messages.

   A TSC that is established between a Communication Manager system and a messaging system will be taken down after the initial message is sent.

4. Set the **SBS** field to `y`.

   The system displays this field only when the **Group Type** field is set to H.323.

5. Set the **Trunk Group for NCA TSC** field to same number as the SBS trunk group.
6. Set the **Trunk Group for Channel Selection** field to the same number as the SBS trunk group.
7. Always set the **TSC Supplementary Service Protocol** field to b.
8. Set the **Near-end /Far-end Listen Ports** fields to equal the far-end value on the distant switch.

   The near-end value on the distant switch must match the far-end value on this near-end switch.

Note:

A signaling group that is used for SBS trunks cannot be used for non-SBS trunk groups. The Near and Far-end Node Names are defined using the change node-names ip administration form.

9. Select **Enter** to save your changes.

Adding trunk group members to SBS trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number.
2. Click **Next** until you see the **Group Member Assignments** section.
3. Add trunk group members to the numbered **Group Member Assignments**.

   This signaling group is used only for SBS signaling.

   Note:

   A signaling group cannot be used for both SBS and non-SBS trunk groups. A SBS trunk group cannot be associated with a signaling group that is connected to a Remote Office.

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

   Note:

   Like standard IP trunks the initial input for the **Port** field should be IP. Once the form has been successfully submitted the actual port information will be shown.

Administering routing for SBS

About this task

Routing at each node occurs through AAR, ARS, and UDP. Calls to nodes using SBS trunking are initially steered to the SBS trunk group for the target (terminating) node. When the SBS Terminating Node returns a complete number to the SBS Originating Node the bearer call is established using ARS and the call is transported over standard bearer facilities (not the SBS trunk group). The bearer always originates through ARS but the complete number may be modified and passed to other routing capabilities (AAR or UDP) and sent through private facilities.

Procedure

1. In a SAT session, enter `change route-pattern n`, where *n* is the number of the route pattern.
2. Set the **TSC** field to `y` for the route pattern to which the SBS signaling calls are directed.

   If the **TSC** field is set to n, Message Waiting Indication (MWI) messages will fail and the voice messaging system cannot light or retire message waiting lamps on individual stations.

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

SBS extension administration

The SBS Extension is an extension type that is translated at each SBS Terminating Node. Each SBS Extension must be Direct Inward Dial/Direct Dial In (DID/DDI) accessible at the SBS Terminating Node it is administered on. However, if the bearer call arrives at the SBS Terminating Node through other than PSTN DID/DDI trunks, for example private Tie Trunks, the SBS feature does not require that the SBS Terminating Node have physical DID/DDI trunks. You must allocate sufficient SBS Extensions for the expected SBS traffic volume.

Note:

SBS Extensions are only in use for the duration of call setup, not for the entire duration of the SBS call.

The SBS Extension type emulates a station with three call appearances. You cannot assign a coverage path or station hunting for an SBS Extension.

Adding an SBS station extension

Procedure

1. In a SAT session, enter `change station n`, where *n* is a valid extension that is DID/DDI accessible.
2. Set the **Type** field to `sbs`.

   The **Port** field sets automatically to x when **Type** field is set to SBS.
3. Type the name of the extension in the free form **Name** field.
4. Type the tenant number in the **TN** field.

   SBS Extensions may be partitioned through the Tenant Partitioning feature.
5. Type in the Class of Restriction number in the **COR** field.
6. Type in the Class of Service number in the **COS** field.
7. Select **Enter** to save your changes.

Note:

SBS extensions are not real extensions. SBS extensions should not be entered in fields, not other administration forms, where Communication Manager administration expects a real extension. Calls to the SBS extension will fail if you enter SBS extensions on administration forms. Also, such non-SBS usage could disrupt completion of incoming SBS calls (that is, if an SBS Extension was unavailable when needed due to misuse). Examples of fields where an SBS Extension should not be administered include:

- Hunt group member
- Point in a coverage path
- Cover Answer Group member

- Termination Extension Group member
- Hunt-to extension in Station Hunting
- Extension tracked by a **Facility Busy Indicator** button

This list is not exhaustive.

SBS extension mapping

You must define the dial plan on the local system and map the SBS extensions to complete numbers.

Defining the dial plan for SBS extensions

Procedure

1. Enter `change dialplan analysis`.
2. Type in the appropriate extensions lengths according to your dial plan.
3. Select **Enter** to save your changes.

Mapping SBS Extensions to complete numbers

Procedure

1. Enter `change isdn public-unknown-numbering`.
2. In the **Ext Len** field, type the extension length of the extensions in your dial plan.
3. In the **Ext Code** field, type the extension code for each extension.
4. In the **CPN Prefix** field, type the CPN prefix for each extension.
5. Select **Enter** to save your changes.

Map SBS Extensions to Complete Numbers Example

You must map SBS Extensions to a complete number, that is, `area/city/SBS` extension, at each SBS Terminating Node. This complete number is then sent to the SBS Originating Node where ARS establishes the bearer call.

When a SBS call is received, and routes to a local endpoint or non-SBS trunk, an SBS extension is allocated for use during call setup. For example, if the extension was 694102, call processing would index the public-unknown-numbering table for the best match to the extension using the **Ext Code** column.

For example if the best match to the extension is the 6 digit entry for Extension Code 69 and CPN Prefix entry 3034. Call processing takes the associated CPN prefix entry (3034) and pre-pends it to the extension to make a Complete Number, 3034694102. Call processing then pre-pends the local country code to the number, for example, 13034694102.

This complete number is sent to the SBS Originating Node on the SBS trunk that is originating the call.

Note:

The Complete Number that is sent to the SBS Originating Node must be DID/DDI accessible at the SBS Terminating Node. The SBS Originating Node uses its international access code to dial the Complete Number if the local country code provided differs from the local country code of the SBS Originating Node.

Verifying SBS system capacities

About this task

SBS Extensions and trunks count against the pool of available ports and trunks. You must consider whether SBS trunks that you add to an existing system increase traffic on the PSTN trunks. SBS trunk group members count against the pool of available IP trunks. SBS bearer calls usually use the same trunks as normal local and/or toll PSTN calls. Implementation of the SBS feature might require that you increase the quantity of trunks to the PSTN.

Procedure

1. Enter `display capacities`.
2. Scroll through the System Capacity screens until you see the **Voice Terminals** fields.
3. Verify the Used, Available, and System Limit capacities for the **SBS Trunks** field.

   SBS Trunks count against the system maximums for the following trunk ports fields:

   - **Maximum ports** field (Optional Features screen)
   - **Trunk Ports** field (System Capacity screen)
   - **IP Trunks** field (System Capacity screen)
   - **Station and Trunk Ports** field (System Capacity screen)
4. Scroll through the System Capacity screens until you see the **Total Subscribed Ports** fields.
5. Verify the Used, Available, and System Limit capacities for the **SBS Stations** field.

   SBS Stations count against the system maximums for the following trunk ports and stations fields:

   - **Maximum Ports** field (Optional Features screen)
   - **Extensions** field (System Capacity screen)
   - **Stations Records** field (System Capacity screen)
   - **Stations without ports** field (System Capacity screen)
   - **Station and Trunk Ports** field (System Capacity screen)
6. Select **Enter** to exit the screen.

Considerations for Separation of Bearer and Signaling

This section provides information about how the Separation of Bearer and Signaling (SBS) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Separation of Bearer and Signaling under all conditions. The following considerations apply to Separation of Bearer and Signaling:

Call Detail Recording (CDR)

CDR functionality records the calling and the called number information, and the start and end times of each measured call. You administer this CDR functionality on a trunk-group basis within Communication Manager. At the end of a call, the information is made available to an adjunct server for functions such as costing, reports, and traffic analysis.

In the case of an SBS call, the data that is gathered and made available to the adjunct server does not change. However, since each trunk group that is involved in an SBS call can be administered to generate CDR reports, the system can generate two CDR records for each SBS call. The system generates one record for the SBS signaling call, and one record for the SBS bearer call.You cannot link the separate SBS signaling and bearer CDR records.

Since the signaling and bearer CDR records cannot be linked, you might prefer to measure only the bearer calls. The service provider is more likely to bill for the bearer calls. However, note that the SBS bearer call is always answered by the SBS extension, even though the actual called party does not answer the SBS call. The parties on the SBS bearer call are not the actual originating and terminating parties. The parties on the SBS bearer calls are dummy users, who are internal to Communication Manager for the sole purpose of originating and terminating the bearer call.

Call Management System (CMS) and Basic Call Management System (BCMS)

You can administer the following entities to be measured for CMS or BCMS:

- A trunk group
- A Vector Directory Number (VDN)
- A hunt group

An SBS call can generate two separate CMS or BCMS records. The system can generate one record for the SBS signaling call, and one record for the SBS bearer call.

CMS and BCMS measure the SBS bearer call only if the bearer trunk group is administered to be measured. CMS and BCMS measure only the trunk bearer seize events and idle events.

The SBS signaling call is measured if the SBS signaling group is administered to be measured, or an endpoint on the SBS call is a measured object. A measured object can be an agent in a hunt group that is administered to be measured. The measured events on the SBS signaling call include not only the trunk signaling seize events and idled events, but also any endpoint events, such as agent hold.

The SBS signaling and bearer calls generate separate CMS or BCMS records with different Universal Call IDs (UCIDs). You cannot link these separate records.

Calling Party—Delay in Call Setup Time

When originating an SBS call, the calling party might perceive a delay in call setup time compared to non-separated calls. This delay is caused by several factors. First, the SBS bearer call cannot be initiated until after the SBS signaling call initiates and a number to route the SBS bearer call to is received from the SBS Terminating Node. Then, the establishment of this SBS bearer call may

be noticeably delayed relative to a non-SBS call, depending upon the type of bearer trunk selected and its trunk signaling protocol. Finally, DTMF digits must be sent over the SBS bearer call, so that the SBS Terminating Node can identify the correct bearer call, which also adds delay.

The exact amount of these delays depends upon several variables such as the amount of congestion in the IP network used for the SBS signaling call and the type of bearer trunk used for the SBS bearer call.

Given a fairly un-congested data network, SBS calls add approximately 1.5 seconds to the call setup time as perceived by the originating user. The SBS delay of approximately does not affect the originating user in any profound way. This delay is relative to a non-separated call over the same type of trunk as used for the SBS bearer call.

The time before the originator hears audible ringback may approach 10 seconds for a bearer trunk that is slow to outpulse digits (rotary). However, a non-separated call using the same bearer trunk would result in a delay of approximately 8.5 seconds before audible ringback is heard. Some bearer trunks can outpulse digits quickly. An example of message oriented signaling trunks is ISDN. For these types of bearers, the SBS induced delay is a majority of the overall delay until the originator hears audible ringback.

The called party will perceive no delays relative to non-separated calls. All setup, validation, and association of SBS signaling and bearer calls occur before alerting of the called party.

Feature Information Displays

SBS call display feature information such as Name and Number, call transfer or forward indication and transfer-to or forward-to party information is the same as QSIG calls. SBS call displays are driven exclusively by translations and signaling on the SBS trunk, and not by translations/signaling on the associated bearer trunk.

Interactions for Separation of Bearer and Signaling

This section provides information about how the Separation of Bearer and Signaling (SBS) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Separation of Bearer and Signaling in any feature configuration.

Overview of SBS interactions

SBS provides a separated trunk call. Many types of trunks can be used to carry the bearer portion of the separated call. Thus, SBS affects many Communication Manager features. Almost any feature that can interact with a trunk call can interact with SBS.

This section describes features that might interact with SBS calls. Other features might also interact with SBS in a minor way.

You must understand how SBS calls are configured internally to understand why certain features can work with SBS calls, and others cannot. This general understanding also helps you to accurately predict whether a feature that is not included in this section can successfully work with an SBS call.

Two important facts about the internal configuration of an SBS call are:

- SBS bearer and SBS signaling calls are tracked internally as separate calls for the life of the SBS call. Separate call records are created internally for each call to:
  - Allow the SBS bearer call to be carried over almost any type of trunk
  - Use the standard call establishment and tear-down code for that trunk type

    The system cannot use the standard code if the bearer trunk is somehow buried as a nonstandard party in a merged signaling and bearer call record.
- The endpoint users are parties on the SBS signaling call, and not on the SBS bearer call. In other words, the SBS signaling call controls the call. Endpoint user activity drives QSIG signaling only if a QSIG trunk is a party on the call. Therefore, the SBS signaling call must control the call. A QSIG trunk is guaranteed only if the endpoint user is associated with the SBS trunk. A QSIG trunk is not guaranteed if the endpoint user is associated with the bearer trunk.

Potential SBS interactions

Based on these two facts about the internal configuration of an SBS call, the following general observations about feature interactions with SBS calls can be made.

Most features work with SBS

A significant number of the features that can interact with an SBS call work as those features do with any other QSIG trunk call.

Delay applies to all SBS calls

For features that do work with SBS calls, the standard SBS delay applies. However, some of the following feature interaction descriptions do not specifically mention SBS delay.

Call status

Any query or report that is related to an endpoint user on an SBS call indicates the call ID of the SBS signaling call, and the trunk ID of the signaling trunk, but not the bearer trunk. For example, a **`status station`** command that is issued against a telephone on an SBS call shows the telephone that is connected to an SBS trunk.

Feature signaling interworks to and from SBS signaling calls

Any feature information that is interworked from a non-SBS leg of a call to an SBS leg of a call is transported on the SBS signaling call, and not on the SBS bearer call. Likewise, any feature information that is interworked from an SBS leg of a call to a non-SBS leg of a call is taken from the SBS signaling call, and not from the SBS bearer call.

Two records per SBS call

Any feature that reports or records status for a call can create two different reports or records for a single SBS call. The feature can create one report or record for the signaling trunk, and a second report or record for the bearer trunk. For example, with Call Detail Recording (CDR), the number of reports or records depends on whether both trunks groups are administered to produce call detail records.

Bearer trunk signaling features

Features that require signaling over a non-QSIG type of trunk do not work with SBS calls. The endpoint users are not parties on the SBS bearer call. Therefore, user activity cannot drive any feature signaling on the bearer call. Similarly, any feature signaling that is received on the bearer call cannot drive any notification or displays to the endpoint user. For example, public or private network-specific (non-QSIG) Malicious Call Trace (MCT) network notification and Advice of Charge (AOC) display functionality do not work with SBS calls.

Bearer trunk user features

Features that are related to the SBS bearer call and require activation or acknowledgement from an endpoint user do not work with SBS calls. Such features do not work with SBS calls because the endpoint user is not a party on the bearer call. For example, queuing of the SBS bearer call does not work because the real originating party is not on the bearer call.

Early-answer features

Features that require early answer do not work with SBS calls. Such features do not work with SBS calls because when the signaling call is answered, the bearer call is not started. When the bearer call is first answered, the call is for the SBS extension at the terminating node. For example, authorization code collection on incoming calls and direct calls to remote access does not work with SBS calls.

Network features that send tones when the bearer call answers do not work

Network features that send tones when the bearer call answers do not work with SBS. When the bearer call is answered, the call is for the SBS extension. The final telephone user is not on the call to hear the tones. For example, the user does not hear the dual-tone multifrequency (DTMF) notification when a network call is eligible to be transferred, such as with Take-back and Transfer.

General system features and SBS interactions

- Media processor resources are not used by the SBS trunks. SBS trunks carry only SBS signaling calls. SBS bearer calls require media processor resources if IP trunks are used.

  Voice quality can degrade if you use IP trunks for bearer calls.
- Shuffling and hairpinning work with SBS bearer calls if you use IP trunks. The SBS bearer call originates with the same shufflable endpoint characteristics as the originator.
- The system obtains the contents of the Incoming Call Identification (ICI) display for an SBS call from the SBS signaling call, and not from the bearer call.
- The system uses the Class of Restriction (COR) of the SBS call originator to set up the SBS bearer call.
- The system routes the SBS signaling and bearer calls separately. Use caution when you administer Toll Restriction, Toll Analysis, and Toll/Code restriction so that you do not block calls that should be allowed.
- The Class of Service (COS) Trunk-to-Trunk Transfer permission affects the transfer of SBS trunk calls in the same way as for non-SBS trunk calls.
- SBS calls follow the Station Hunting of the originally called party.

- When Tenant Partitioning is active in an enterprise, existing Tenant Partitioning rules apply to endpoints, SBS extensions, SBS trunk groups, and the bearer trunk groups that are involved in any SBS call.
- SBS works with Dial Plan Expansion of 6-digit or 7-digit extensions.
- Standard Malicious Call Trace (MCT) on an incoming SBS call records the bearer trunk call.

Attendant interactions with SBS

Attendant features that do not work with SBS

- Attendant Control of Trunk Group Access does not work with an SBS Trunk Group.
- Centralized Attendant Service (CAS) does not work over SBS trunks, since CAS requires release link trunks (RLT). However, you can use CAS to direct an incoming SBS call to a centralized attendant over an RLT. Likewise, a centralized attendant can extend a call over an RLT, that the system then routes to an SBS trunk.

Attendant features that work with SBS

- Attendant Direct Extension Selection (DXS) can be used to originate an SBS call that uses Uniform Dial Plan (UDP).
- Attendant Intrusion can be used to intrude on an SBS call.
- Attendant Recall works with an SBS call
- Attendant Return Call and Serial Calling work with an incoming SBS call.
- Attendant transfer is applicable to an SBS call.
- An incoming SBS call can be parked, and is subject to Call Park Time-out to the Attendant.
- An SBS call can be a party in an attendant conference.
- An SBS call can be directed to an individual attendant access number.
- Inter-PBX attendant service works with SBS trunks.
- Incoming SBS calls follow attendant Night Service.
- Incoming SBS calls hear Recorded Announcements in the attendant queue.
- You can use Trunk Answer Any Station (TAAS) to answer an incoming SBS call.
- The Trunk Identification by Attendant feature identifies the SBS trunk group member.
- An SBS call can be held with Two-Party Hold on Console.
- Attendant Vectoring can receive and redirect attendant-directed calls over SBS trunks.

Adjunct Switch Applications Interface interactions with SBS

- When you use Call Classification after Answer, do not use SBS to route calls. Do not use SBS because the Call Classifier must be on the bearer trunk, and the SBS-invoked DTMF signaling that is sent on the bearer trunk causes interferences.

- Adjunct Switch Applications Interface (ASAI) Phantom call, such as DEFINITY Anywhere, can originate or receive an SBS call.
- ASAI Selective Listening works on an SBS trunk party on a call.
- ASAI Send DTMF works on a connected SBS call.
- ASAI Single Step Conference can add another station onto a call with an SBS call.
- ASAI Provided Dial-Ahead Digits work when the incoming call is an SBS call.
- Any ASAI user data, Universal Call ID, or both that are currently transported or interworked over QSIG trunks, are sent on the SBS signaling call.
- Any II Digits that are received in the SETUP message to the incoming SBS Signaling call are tandemed with the SBS signaling call when an SBS call is received and subsequently tandemed over an SBS trunk.
- The information that is provided in response to an ASAI Value Query indicates whether an SBS trunk or an associated bearer trunk is idle or busy. The response is based on the UID in the query message and whether the response was for the signaling or the bearer trunk.
- For ASAI Event Reports, Communication Manager reports the Call ID and the Trunk ID of the SBS trunk. ASAI provides the Trunk ID of the associated bearer trunk to the ASAI Event Reports and Adjunct Route message.

Communication Manager Messaging and Octel voice mail adjuncts interactions with SBS

- Centralized voice mail with Interswitch Mode Codes does not interwork with SBS trunks. For that application, the tie trunks between the servers that run Communication Manager cannot use the QSIG protocol. While those tie trunks might be used for SBS bearer calls, SBS is likely not implemented when this methodology is used.
- Leave Word Calling with Message Wait Indicator over QSIG (QSIG LWC MSI) uses SBS to support Digital Line Emulation integration for centralized voice mail.
- SBS supports centralized Communication Manager Messaging from a served user switch.
- Where an Octel Serenade is connected to Communication Manager with QSIG, the server that runs Communication Manager is the SBS terminating node. This SBS terminating node interworks to the Serenade, since the Serenade does not support SBS.

Call Center interactions with SBS

Automatic Call Distribution interactions with SBS

- Look Ahead Interflow (LAI) might not function correctly on an SBS call, because of the SBS call setup delay. If the SBS delays are a problem, you might use Non Call Associated (NCA) Temporary Signaling Connection (TSC) instead of LAI to poll by Best Service Routing (BSR).
- Normal SBS call setup delays affect calls if Outbound Calling is done from a Call Center, and the call uses SBS to call another Communication Manager system. Outbound Calling over SBS trunks must not use Call Classification. Outbound Calling will have interference from

the DTMF signaling that is invoked by SBS and sent to identify the correct bearer call at the terminating end.

- Dialed Number Information Service (DNIS) and Original Dial Number Delivery service from a service provider can deliver an SBS bearer call to an SBS extension in an SBS terminating node.
- When an incoming Automatic Call Distribution (ACD) call arrives by way of an SBS trunk, transfers by an agent to another agent or to an application work properly.
- An incoming SBS call can hear any announcements that are associated with the Call Center.
- The Agent Assist functionality works when the incoming call arrives over SBS.
- Displays at the agent terminals function correctly when the incoming call arrives over SBS. This includes Vector Collected digits.
- Multiple Call Handling works when arriving calls are incoming SBS calls.
- An incoming SBS call that receives Redirect on No Answer (RONA) works correctly.
- SBS calls that receive intraflow, interflow, or hunt group night service treatment are routed in the same way as a non-SBS call.
- Any ISDN call data, R2MFC call data, or both ISDN and R2MFC data that is currently interworked to or from a QSIG trunk is sent on (retrieved from) the SBS signaling call at the SBS interworking node. Such call data includes calling party number, II Digits, CINFO digits, and so on.
- Call Center data that is currently transported on QSIG trunks is sent on the SBS signaling call.
- When an ACD call is transferred to an agent through an SBS trunk connection on another system that runs Communication Manager, all associated call information that is currently transported on a QSIG trunk is sent on the SBS signaling call.
- All types of Service Observing functions work on SBS calls in the same way as for non-SBS calls.

Best Service Routing interactions with SBS

- Polling by Best Service Routing (BSR) can use SBS signaling facilities when the NCA-TSC version of BSR Polling is used, and adequate resources are available. The non-NCA-TSC version of BSR Polling might not work because of the SBS call setup delays.
- BSR interflow over SBS trunks, including incoming call data forwarding and Enhanced Information Forwarding, are supported.

Vectors interactions with SBS

- Routing on Automatic Number Identification (ANI) by a vector can use SBS to route an outgoing call. For an incoming SBS call, the Routing on ANI functionality uses the ANI from the SBS signaling call.
- Correct routing over SBS trunks works when a vector step exists for routing on ANI or II digits, or a route-to number step, and interflow is invoked.

- Post-Connect in-band DTMF signaling for Call Prompting collect steps and Auto Attendant functionality both work with SBS.
- When CINFO Digit Routing occurs, and the call is routed over an SBS trunk, the information is tandemed with the call.
- Vector Routing Tables can use SBS trunks to route calls.
- Incoming SBS calls still provide VDN of Origin announcements (VOA) and displays to the agent who answers the call.
- VDN Return Destination works with SBS calls.

Networking-related interactions with SBS

Networking features or capabilities that do not work with SBS

- Authorization codes cannot be collected on an incoming SBS signaling call or on an SBS bearer call. Such codes might be required to administer of the incoming trunk group or because of insufficient Facilities Restriction Level (FRL) on a tandem call. Authorization codes cannot be collected on incoming SBS signaling calls for two reasons:
  - The SBS bearer call is not established at the time that the system usually prompts for and signals an authorization code.
  - The originating endpoint user is not a party on the SBS bearer call.
- When the bearer call is transported through Message Oriented Signaling trunks ISDN, information in the SBS bearer call D-channel is not displayed to the end users. The information is not displayed because the signaling in the SBS signaling call overwrites the information.
- User information in the SBS bearer leg of the call is ignored.
- Australian Malicious Call Trace (MCT) cannot be invoked on an SBS call because:
  - End-user activity drives feature signaling only on the SBS signaling call, and not on the SBS bearer call
  - An SBS trunk does not support the Australia public network protocol

  The normal MCT feature within Communication Manager records the call as usual.
- ETSI MCT cannot be invoked on an SBS call because:
  - End-user activity drives feature signaling only on the SBS signaling call, and not on the SBS bearer call
  - An SBS trunk does not support ETSI protocol

    The normal MCT feature within Communication Manager records the call as usual.
- Calling Line ID Prefix information is ignored when the information is transported in conjunction with an associated bearer trunk.

- Advice of Charge (AOC) information that is received on an SBS bearer call is not displayed to the end user. However, AOC information is conveyed to the CDR port for the SBS bearer call record. Only SBS trunk information affects end-user displays.
- ETSI Network Call Deflection (NCD) does not work with an SBS call. For SBS, the signaling that controls the call is in the SBS signaling call on the QSIG interface. NCD, however, requires an ETSI interface that is available only on SBS bearer calls.
- ETSI Network Call Transfer (NCT) does not work with an SBS call. For SBS, the signaling that controls the call is in the SBS Signaling call on a QSIG interface. NCT, however, requires an ETSI interface that is available only on the SBS bearer call.
- Direct SBS calling into Remote Access does not work. Barrier Codes cannot be collected for SBS calls to Remote Access because the SBS bearer call has not yet been established when such tones are prompted for or expected. However, an SBS call can invoke Remote Access by means of a vector collect or a route-to command.
- SBS does not support Wideband Switching (NxDSO).
- Russian Incoming ANI with a button does not display the ANI that is received in the SBS bearer call. The system displays to the end user only the ANI that is received on the SBS signaling call.
- Trunk Flash to get recall dial tone from a central office (CO) does not work. End-user activity drives signaling on the SBS signaling call only, and not on the SBS bearer call. QSIG Call Transfer functionality can be used instead.
- R2 MultiFrequency Compelled (MFC) Intercept treatment must drop the SBS bearer and SBS signaling calls, and does so by applying the appropriate treatment to the call originator based on what is received on the R2 MFC bearer call.

Networking features or capabilities that work with SBS

- When authorization codes are required to access the SBS trunk, authorization codes can be collected. The reason is that authorization codes are collected locally before the outgoing trunk is seized.
- Calling Party Number (CPN) restriction can be administered for and signaled on both the SBS signaling and SBS bearer calls. However, end-user displays, including any restrictions, are populated from information that is carried in the SBS signaling call, and not from information in the SBS bearer call.
- At an SBS Interworking node, DCS and DCS+ signaling on the non-SBS portion of the call is interworked to and from the SBS signaling call, to the extent that DCS-QSIG interworking currently applies.
- A DCS trunk can be used as the bearer trunk on an SBS call. However, any DCS signaling information received on the Bearer call is overridden by the QSIG signaling information received on the SBS signaling call.
- User information that is received on an SBS signaling call by an SBS tandem node, or received on a non-SBS trunk by an SBS interworking node, is sent on the SBS signaling call, per current tandeming or interworking procedures on QSIG trunks.

- Temporary Signaling Connection (TSC) messages can be sent over an SBS trunk.
- Look Ahead Routing can be used with both SBS signaling and SBS bearer calls, if such calls start on ISDN trunks.
- In regions where Feature Plus (F+) is offered, SBS calls can use the pseudo-DID functionality of F+. Then, you do not need to obtain direct inward dialing (DID) or DDI numbers from a service provider. You must administer SBS extensions at the SBS terminating node, but these numbers do not need to correspond with real DID or DDI numbers. CPN prefix administration at the SBS terminating node must map the SBS extension to a number that is a national complete number,. Except, the SBS extension portion is not recognized by the PSTN. ARS at the SBS originating node must route this number to a route pattern preference that supports F+. The “No. Dgts SubAddress” administration for this preference must indicate the length of the SBS extension at the SBS terminating node. This number is the number of digits that are extracted from right to left, and sent in the Calling Party Subaddress Information Element. Administration for this preference must also delete the SBS extension digits, and insert the Listed Directory Number (LDN) extension of the SBS terminating node in its place. The SBS bearer call is routed to the LDN at the SBS terminating node. F+ functionality at the SBS terminating node then routes the call to the SBS extension that is passed in the Subaddress IE, instead of to the attendant. Multiple route patterns are needed at the SBS originating node, if the SBS terminating node uses SBS extensions of various lengths.

  SBS extensions that are used with F+ cannot be longer than 5 digits, because F+ is not included in Dial Plan Expansion.
- QSIG MSI messages are sent in the SBS Signaling link. The system ignores any messages that are in the SBS bearer call.
- QSIG Call Completion works with SBS calls.

  Both the original call and the call-back call incur separate SBS delays if the call uses SBS trunks.
- QSIG Call Transfer works with SBS calls.

  Both the original call and the second call to the transferred-to party incur separate SBS delays if the call uses SBS trunks.
- QSIG Diversion, forward switch and reroute, works with SBS calls.

  Both the original call and the second call, to the forwarded-to party, incur separate SBS delays if the call uses SBS trunks.
- QSIG Path Replacement works with SBS calls.

  The entire SBS call, both the SBS signaling call and the associated SBS bearer call, are replaced. All separate calls, the original call, the call to the transferred-to party, and then the path replacement call, incur separate SBS delays if the calls use SBS trunks.
- QSIG Enhanced Path Replacement works with SBS calls. Multiple SBS delays apply.
- Non-Avaya QSIG MSI are tandemed to and from any non-SBS QSIG portion of an SBS call (at the SBS interworking node) and on the SBS signaling call (at an SBS tandem node) per existing QSIG transit operation.

- QSIG MWI works with SBS calls.
- QSIG Temporary Signaling Connections (TSCs), known as Call Independent Signaling Connections (CISCs) in QSIG literature, are supported. Non Call Associated Temporary Signaling Connections (NCA TSCs) are signaling-only connections that transport feature information. While NCA TSCs can be initiated as a result of some activity on a bearer call, NCA TSCs are independent of bearer calls. NCA TSCs are set up as nonbearer calls, and use a call reference value (CRV) that is different than any CRV that is in use on any other existing bearer or signaling call on that interface.

  Communication Manager supports two different NCA TSC protocols. Use the signaling group **TSC Supplementary Service Protocol** field on the Signaling Group screen to administer these protocols. The **TSC Supplementary Service Protocol** field is set to a for AT&T NCA TSCs, and to b for QSIG NCA TSCs (CISCs).

  For full QSIG functionality, you must set the **Supplementary Service Protocol** field on both the Trunk Group screen and the Signaling Group screen to b (QSIG). You must set this field to b, because some QSIG features, such as QSIG Call Completion and QSIG Message Waiting Indication, use QSIG feature signaling on both the bearer call and on an NCA TSC to work properly.
- QSIG Centralized Attendant Service with MSI works with SBS calls.
- QSIG transit capabilities are supported with SBS calls through tandeming of QSIG signaling to and from any non-SBS QSIG portion of an SBS call (at the SBS interworking node), and on the SBS signaling call (at an SBS tandem node), per existing QSIG transit operation.
- QSIG VALU signaling works with SBS calls. You might need to increase the timer that is used to return QSIG VALU Call Coverage calls back when the calls are unanswered, so that SBS delays do not cause such calls to be returned prematurely. Use the **Local Cvg Subsequent Redirection/CFWD No An Interval (rings)** field on the System Parameters Call Coverage/ Call Forwarding screen to administer the timer.
- QSIG Called/Busy Name ID is supported in the SBS signaling call.
- QSIG Calling/Connected Name/Number ID is supported in the SBS signaling call.
- QSIG Call Offer is supported in the same way as over normal QSIG trunks.
- Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), or both AAR and ARS can be used to route the SBS signaling call. SBS bearer calls are routed by ARS only, but also can be directed to AAR from ARS.
- SBS calls to an analog station endpoint display the SBS signaling information if the endpoint is served by a MM711 port.
- The Russian Transit/Power Industry Tie Trunk is expected to work as an associated bearer trunk.
- The X-Station Mobility feature works for incoming or outgoing calls that are routed with SBS.
- Leave Word Calling (LWC) for Unanswered External Calls with Automatic Number Identification (ANI) is supported with the information in the SBS signaling call that is stored for the called party.

- ISDN Feature Plus calls are supported, as the SBS bearer call, with the SBS signaling call information that is used for endpoint displays.
- ISDN Calling Party Number Presentation options are supported by SBS in the SBS signaling call.
- QSIG/DCS Partial Reroute works is the same way as it does currently, with the SBS signaling call as the QSIG part of the call.
- DS1 With Echo Cancellation is supported for the SBS bearer call.

Network interface SBS interactions

- DTMF ANI signaling on an incoming SBS bearer call could interfere with the SBS invoked DTMF signaling set to identify the correct bearer call. This service should not be subscribed to on trunk groups that may be used to deliver SBS bearer calls.
- If you use in-band call transfer capability from a network Service Provider (like Take back and Transfer) and subscribe to a notify option, the incoming DTMF signals on an SBS bearer call will cause the SBS bearer call to fail. This service should not be subscribed to on trunk groups that may be used to deliver SBS bearer calls.
- If you subscribe to Alternate Destination Routing, they must take care to not include the SBS extension numbers in the DID/DDI blocks subject to reroute. If such alternate routing occurs, the incoming SBS bearer call cannot be associated with its SBS signaling call and will be dropped.
- Hong Kong DTMF Supplementary Services information will not be displayed to the endpoint user on an SBS call since the display contains information from the SBS signaling call.
- Macedonia E1 Support for PPM messages will not be displayed to the endpoint user when this type trunk is used as an SBS bearer because bearer trunk signaling does not impact user displays on SBS calls.
- Calling Party Number (CPN) information received on an SBS bearer call will be tandemed on the SBS bearer call but it will not be displayed to the endpoint user. It is available for Call Detail Recording (CDR) on the bearer call record.
- An analog station connected to a MM711 port with Incoming Call ID will see the SBS signaling information when making or receiving an SBS call.
- US Analog Trunk & Line - MM714 - Supports SBS.
- Country specific functionality that does not require end user activation, acknowledgement, or display will be supported on SBS bearer calls. For example, China Disconnect on No-Answer will disconnect the bearer call and the SBS signaling call will also disconnect.
- Disconnect supervision for an SBS bearer call is provided/processed as usual for that type of bearer trunk. If no disconnect supervision is available on a trunk used for an SBS bearer call, then disconnect supervision will be provided by the SBS signaling call. Dropping either the SBS bearer call or the SBS signaling call will drop the associated SBS signaling/bearer call respectively.
- For ISDN trunks, the Incoming Call Handling Table may be used to delete leading digits of the SBS bearer call’s called number to direct the call to the indicated SBS Extension. Digit

manipulation must not modify the extension portion of the number, or the SBS bearer call will not terminate to the indicated SBS Extension and thus cannot be associated with its SBS signaling call.

- For non-ISDN trunks or ISDN bearer trunks using overlap receiving, insertion/deletion may also be used to direct the SBS bearer call to the indicated SBS Extension. Again, digit manipulation must not modify the extension portion of the number, or the SBS bearer call will not terminate to the indicated SBS Extension and thus cannot be associated with its SBS signaling call.
- Where ANI is received on an incoming non-SBS call, and the call is tandemed to another Communication Manager using SBS, the received ANI information will be tandemed in the SBS signaling call to the far end per current QSIG interworking procedures. The network interfaces that may receive ANI and then tandem to a SBS call include:
  - Analog CO Trunk (MM714/MM711)
  - R2-MFC trunks
  - India MFC trunks
  - Integrated R2-MFC Signaling - DID/CO
  - MFE
  - MFC and Russia MF Multiple ANI
  - Spain MFE
- For the No Disconnect Supervision Trunk Operation, the SBS signaling call will control disconnect supervision for the associated bearer call.

Chapter 159: Service Observing

Using the Service Observing feature, designated users can listen to another user calls.

From AE Services Release 8.1.3 and Communication Manager Release 8.1.3 onwards, a new third-party call control support is added for the activation and deactivation of service observe, service observe connection mode change, query service observe status, and monitor service observe the state change, on a hard phone. Service observer state change events are only sent on station monitors if the ASAI version is 12 or later.

Detailed description of Service Observing

This section describes service observing in environments without Automatic Call Distribution (ACD) or call vectoring. To use service observing in ACD or call vectoring environments, see the *Avaya Aura® Call Center Elite Feature Reference*.

With Service Observing, designated users, who are usually supervisors, can listen to other users calls. The user that observes the calls of another user is called an observer. Use the Service Observing feature to train agents, or to monitor the quality of service in call centers and other environments where employees serve customers over the telephone.

Warning:

Listening to the call of another user can be subject to federal, state, or local laws, rules, or regulations. You might need to obtain the consent of one or both of the parties on the call. Ensure that you know, and comply with, all applicable laws, rules, and regulations when you use this feature.

An observer can monitor calls to any of the following entities:

- An extension
- A vector directory number (VDN), on systems with call vectoring
- A logical agent ID, on systems with Expert Agent Selection (EAS)

Observers can monitor calls in listen-only mode or listen-and-talk mode. In listen-and-talk mode, an observer can hear and speak with all parties on a call. The user that is monitored does not know that an observer listens to the call, unless you administer Communication Manager to provide a monitoring tone.

When an observer is off-site, the observers can use remote access to monitor calls. In systems with call vectoring, a vector can control access to Service Observing.

If an observer uses a telephone that has a service observe button, the button:

- Blinks while the observer waits for an eligible call
- Lights steadily while the observer observes a call

The system does not reserve a call appearance while the observer is in the wait state, if:

- The observer uses a Feature Access Code (FAC) to activate Service Observing
- No service observe button is administered for the telephone

An idle call appearance must be available for an observer to go to the observing state when an eligible call arrives.

Service Observing Listen and talk modes

When an observer uses the feature button for Service Observing, the observer can toggle between listen-and-talk mode and listen-only mode. However, when an observer activates Service Observing with an FAC, the observer must choose the listen-only mode or the listen-and-talk mode at the start of the session. If the user wants to change modes after the session starts, the observer must end the session, and then choose the other mode when the observer starts a new session. The FACs for Service Observing are the following:

- Service Observing Listen Only Access Code
- Service Observing Listen/Talk Access Code

Note that the system also requires an FAC for remote Service Observing.

An observer can observe an agent who is not active on a call. The observer is in a wait state until the agent receives a call, and then the observer is bridged onto the call.

Service Observing with Multiple Observers

Service Observing with Multiple Observers means the following:

- Up to two observers can monitor the same agent Login ID or station extension using the Service Observing station button or using any of the following Feature Access Codes (FACs):
  - Service Observing Listen-Only
  - Service Observing Listen/Talk
  - Service Observing No-Talk
- Two separate calls, each with an associated service observer, can be conferenced together with both service observers included in the merged conferenced call except when both observers are VDN observers. In this case, one VDN observer is dropped.
- If you use call recording product, such as the Avaya Witness Call Recording or NICE can connect a voice-storage server to a station or Login ID extension to record agent-to-customer transactions acting as an observer. Priority in call recording observing is given by using the “Service Observing by Recording Device” COR feature, which is specifically added for this purpose. The priority between the recorder and the observer depends on the type of device

registration. The recording device registration type is given higher priority than the observer. The recording device registration uses IP applications and observing devices use IP stations.

- If you use call recording products, you can allow an observer to monitor a station or Login ID extension and record the transaction at the same time.

Note:

This feature restricts multiple observers on the same call for the Service Observing by VDN feature.

Service Observing telephone displays

The system displays the same information for both the user and the local observer. The service observer display shows <origination> to <destination> so <origination> is the Observed Party's information, and <destination> can either be the called-party or a trunk.

Service Observing on trunk calls

When a user places a trunk call, Service Observing starts when the user finishes dialing the call. For calls on central office (CO) trunks, the system considers dialing to be complete when the answer supervision is returned, or when the answer supervision timeout occurs.

The system denies any attempt to use Service Observing over trunks that do not have a disconnect supervision.

Service Observing warning and conference tones

You can administer a tone that notifies the parties on a call that the call is observed. You can administer the tone as a warning tone or a conference tone.

If you administer the tone as a:

- Warning tone, the system generates a unique 2-second, 440-Hz tone before an observer connects to the call. While the call is observed, the system repeats a shorter version of this tone every 12 seconds.
- Conference tone, the system generates the conference tone before an observer connects to the call. The system does not repeat the conference tone during the call.

VDN Observing by Location

Supervisors can use VDN Observing by Location to:

- Dial a Feature Access Code (FAC) to set up an observing association with a VDN that establishes observing connections to calls to the VDN when the agent in the required location answers the call.
- Indicate the location of the agents that the supervisor needs to observe by entering a location ID number of the Multiple Locations feature. Communication Manager connects calls from the supervisor only to the agents who have the assigned location ID number.

You can activate VDN Observing by Location using FACs in the following modes:

- Listen Only: VDN Observing by Location Listen Only Access Code.
- Listen/Talk: VDN Observing by Location Listen/Talk Access Code.

For more information on VDN Observing by Location, see *Avaya Aura® Call Center Elite Feature Reference*.

Support for Service Observe and Barge-in features using feature access code through ASAI

Communication Manager Release 7.1.1 or later enables Avaya Oceana® to:

- Perform Service Observe and Barge-in operations on a voice channel.
- Add a Service Observer to a call by using Feature Access Codes.
- Toggle between listen-only and barge-in modes through CTI. To toggle between modes, Avaya Oceana® must drop a Service Observer while in a mode and add the Service Observer back while in another mode.

Support to drop or disconnect Service Observer from call using CTI application over ASAI

Prior to Communication Manager Release 7.1.1, a Service Observer was dropped or disconnected from a call only when the Service Observer goes on-hook. From Communication Manager Release 7.1.1 onwards, you can drop or disconnect a Service Observer from a call using a CTI application over ASAI.

Service Observing administration

This section describes the screens that you use to administer the Service Observing feature.

Screens for administering Service Observing

Screen name	Purpose	Fields
Class of Restriction	Set up the Class of Restriction (COR) to support Service Observing.	• Can Be Service Observed • Can Be Service Observer • Service Observing COR Table

Table continues…

Screen name	Purpose	Fields
Feature Access Code (FAC)	Specify the FACs for Service Observing.	• Service Observing Listen Only Access Code • Service Observing Listen/Talk Access Code • Service Observing No Talk Access Code • Service observing Next Call Listen Only Access Code • VDN Observing by Location Listen Only Access Code • VDN Observing by Location Listen Only Access Code
Feature-Related System Parameters	Enable Expert Agent Selection (EAS) for the system.	Expert Agent Selection (EAS) Enabled
	Enable a conference tone for observed users.	Service Observing Conference Tone
	Enable a warning tone for observed users.	Service Observing Warning Tone
	Block the service observer from monitoring an agent if the service observer and agent are in different tenant partition groups.	Block Service Observe Across Tenants
Station (multiappearance)	Assign the **serv-obsrv** button for Service Observing.	Any available button field in the **Button Assignment** area
Optional Features	Enable Service Observing for: • Basic or logical agent ID observing • Remote access • Vector Directory Numbers (VDNs) • Vector-initiated observing	• Service Observing (Basic) • Service Observing (Basic) and Service Observing (Remote/By FAC) • Service Observing (Basic) and the Service Observing (VDNs) • Vectoring (Prompting)

End-user procedures for Service Observing

End users must perform specific procedure to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Activating Service Observing

Procedure

1. Press the **serv-obsrv** button for H.323 or **sip-sobsrv** button for supported SIP stations.
2. Dial the extension that you want to observe.

   When you use the **serv-obsrv** button to activate Service Observing, you start in listen-only mode. Press the **serv-obsrv** button to toggle between listen-only mode and listen/talk mode.

Deactivating Service Observing

Procedure

Disconnect the call, select another call appearance, or press the disconnect or release button.

You can also deactivate the Service Observing by pressing the **serv-obsrv** or **sip-sobsrv** button.

Interactions for Service Observing

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

Attendants

An attendant can be observed, but cannot be an observer.

Bridged Appearances

You observe calls on a primary extension and all bridged appearances of that extension. You cannot observe bridged appearances on the extensions 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.

The primary telephone user or bridging user can bridge onto a service observed call of the primary at any time. A bridging user cannot activate Service Observing using a bridged call appearance.

If the primary is service observing on an active call, a bridged call appearance cannot bridge onto the primary line that is doing the service observing.

Busy-Verification

You cannot observe an extension that is being busy-verified. You cannot busy-verify an extension that is being observed.

Call Coverage and Call Pickup

An observer cannot observe a call that is answered by a covering agent or a member of a pickup group, unless the called agent bridges onto the call.

Call Park

An observer cannot park the observed call.

Call Waiting

Incoming calls do not wait on a single-line telephone that is being observed.

Conference

An observer cannot initiate a conference call while the observer is also observing a call.

If an observed user starts a conference, or enters a conference call that has fewer than six parties, the system places the observer in the wait state until the system connects the call. Then the observer can observe the conference. The system counts the observer as one of the conference call participants. The observer can observer all of the conference participants, regardless of the Class of Restriction (COR). In addition, the system bridges the observer onto any calls that a conference participant places or receives while the conference is active. When the user leaves the conference, the observer also leaves and returns to observing the original call.

Note:

For 12 parties to participate in a conference, you must enable the **12–party Conferences** field in the Feature-Related System-Parameters screen.

Data Privacy

An observer cannot observe an extension:

- On which Data Privacy is active
- While the extension is on a conference call with another extension for which Data Privacy is active

Data Restriction

An observer cannot observe an extension

- On which Data Restriction is active.
- While the extension is on a conference call with another extension for which Data Restriction is active

Distributed Communications System (DCS)

To observe user extensions that are on another node, such as a DCS station extension, the observer must set up remote-access service observing.

The system does not transmit service observing displays across DCS networks.

Extension to Cellular

You cannot activate the Service Observe feature from numbers mapped with EC500. If a call comes in from a number mapped with EC500, Communication Manager considers the call to be bridged appearance. If you use bridged call appearance, you cannot use Service Observing.

Hold

An observer cannot place a call on hold while the observer is also observing a call.

If a user who is being observed places a call on hold, the observer enters the wait state.

Integrated Directory

Observers do not hear a user dial an integrated directory number.

IP Solutions

If an observer observes an IP to IP direct call, the users on the call might hear a break-in conversation of about 200 milliseconds.

Leave Word Calling (LWC)

Parties on an observed call cannot use LWC.

Music-on-Hold

If an observer is in listen-talk mode, neither the caller nor the observer hears music-on-hold. If an observer is in listen-only mode, the caller hears music-on-hold, but the observer does not.

Privacy - Manual Exclusion

Observing towards a station with Exclusion active is denied, or if Exclusion is activated by a station while being observed, all bridged parties including the observer are dropped. If the **Service Observing with Exclusion** field on the Feature-Related System Parameters screen is y, then Service Observing of a station with Exclusion active, either by Class Of Service or by manual activation of Exclusion, is allowed.

Transfer

An observer cannot initiate a transfer while the observer is also observing a call.

If a user transfers a call, the observer is placed in the wait state. The observer is bridged onto the call when the transfer is complete.

Chapter 160: SIP and H.323 dual registration

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

Detailed description of SIP and H.323 dual registration

When you use an extension to register a SIP endpoint to Session Manager and an H.323 endpoint to Communication Manager, an incoming call to that extension rings at both the endpoints. The user can answer the call either at the H.323 endpoint or at the SIP endpoint. Calls appear through simulated bridged appearances (SBA) on the other endpoint. You can hand off a call to another endpoint through SBAs or an extend-call button. You can use the following features with a dual-registered extension:

- Video calls
- Mute
- Hold
- Transfer
- Conference
- Initial Direct Media
- Bandwidth management

You can create the extension of H.323 type by using System Manager. You can reassign the same extension as SIP by using the off-pbx-telephone station-mapping screen in Communication Manager SAT.

The following endpoints support SIP and H.323 dual registration:

Note:

You cannot configure the Hunt group position busy button on the dual registration enabled endpoints.

Communication Manager Releases	Audio endpoints	Video endpoints
6.3	• 96xx and 96x1 H.323 and SIP • Avaya one-X® Communicator for Windows H.323 and SIP	—
6.3.x	• 96xx and 96x1 H.323 and SIP • Avaya one-X® Communicator for Windows H.323 and SIP • Avaya one-X® Communicator for Mac OS X SIP iOS	• Avaya Communicator for iPad Devices Release 2.1.03 • Avaya Communicator for Windows Release 2.1.1
7.0 and later	• J100 series • 96xx and 96x1 H.323 and SIP • Avaya one-X® Communicator for Windows H.323 and SIP • Avaya one-X® Communicator for Mac OS X SIP iOS	• Avaya Workplace (formerly Avaya Equinox) • Avaya Communicator for iPad Devices Release 2.1.03 • Avaya Communicator for Windows Release 2.1.1

Limitations of SIP and H.323 dual registration

- Both H.323 and SIP devices do not work with full functionality on Dual Registration. The normal way is to configure the phone as H.323 with a SIP Optim mapping. The other way is to configure the phone as SIP. However, you must prefer one protocol over the other.
  - If you configure the phone as H.323 with a SIP Optim mapping, the H.323 phone works with full functionality. In this scenario, the SIP phone may lack some features.
  - If you configure the phone as SIP, the SIP phone works with full functionality. In this scenario, the H.323 phone may lack some features.
- If you are migrating from H.323 to SIP and if you want the SIP phone to work with full functionality, then you must reconfigure the phone as SIP. In this scenario, the H.323 phone gets reduced functionality as described elsewhere in this section.
- If the H.323 phone and the SIP phone are on the same call and if a user presses the **drop** button on one of the phones, the call is dropped from both the phones.

  Note:

  Instead of using the **drop** button, if the user goes on hook from one of the phones, the call remains active on the other phone.
- When an endpoint is configured using dual registration, some of the Equinox features do not work. To overcome this, you must configure the endpoint as SIP. If multiple SIP devices are required, then you *must* use Multiple Device Access (MDA) instead of dual registration.

- When a Dual Registration user places a call using the SIP device, the H.323 device does not display a Bridge soft key. Instead the H.323 device shows soft keys for hold, conference, transfer, and drop. To join the call, the user needs to either press the button next to the call appearance or the **OK** button on the H.323 phone.
- When a Dual Registration user makes an outgoing call on the H.323 device, the SIP endpoint shows the Bridge soft key without the hold, conference, transfer, and drop soft keys.

  Note:

  If the SIP user sets the call on hold or unhold, all the soft keys disappear and the soft key for bridge appears on the screen.
- No feature activation is supported while the SIP and H.323 endpoints are on the same call.
- When a paging group receives a call, the H.323 phone goes on speaker and a one-way talk path is established from the called party to the H.323 phone. The speaker on the SIP phone is not activated, but the SIP phone can bridge on to the call. If the caller bridges on to the call from the SIP phone, a two-way talk path is established between the calling party and the SIP phone.
- If a call is answered by the H.323 phone, the call log on the SIP phone shows a missed call entry.
- If the H.323 phone bridges on to the existing call, the soft buttons for hold, conf, transfer, and end call appear on the phone. These soft buttons appear on the phone even when the H.323 phone goes off hook.

  Note:

  You can rejoin the bridge by using the **OK** button on the hand set.
- The H.323 telephone can bridge onto the call by selecting the simulated bridge appearance. The system does not support bridging if Exclusion is active. While the dual registered SIP and H.323 endpoints are both bridged onto the same call, the system does not support any feature usage affecting that call.
- SIP and H.323 endpoints with a dual registered extension do not support the call transfer functionality. However, when you activate this feature from H.323, transfer recall works as expected. Both the endpoints ring after transfer recall timer expires.
- The following features are not supported on a dual registered extension:
  - Speakerphone paging
  - Automatic exclusion
  - PSA disassociated FAC

Note:

The limitations in the preceding list are not exhaustive and might vary from system to system. All feature operations not explicitly stated in this chapter are not supported in a dual registration configuration. For example, dual-registered endpoints in a contact center is not

supported. For further assistance with the feature administration and caveats, raise a service request at https://support.avaya.com/.

Screen for administering SIP and H.323 dual registration

Screen Name	Purpose	Fields
Stations With Off-Pbx Telephone Integration	To add an OPS entry on Communication Manager	• Application • Dial Prefix • Phone Number • Trunk Selection • Config Set

Administering SIP and H.323 dual registration

Procedure

Do the following:

a. Through System Manager, create an extension of H.323 set type, and select the **Allow H.323 and SIP Endpoint Dual Registration** check box.

b. To enable dual registration, you can manually add H.323 stations on Communication Manager and then add OPS entries for the added stations. This method is time consuming for large number of stations. To overcome this problem, you can perform bulk addition of SIP stations.

Interactions for SIP and H.323 dual registration

Multiple simultaneous calls

H.323 endpoint and SIP endpoint with a dual registered extension support multiple simultaneous active calls.

H.323 SBA for OPS call

H.323 deskphones support simulated bridged appearance for OPS calls. When a SIP endpoint is active on a call, H.323 desk telephone shows the call as a simulated bridge appearance. The H.323 telephone can bridge onto the call by selecting the simulated bridge appearance. The system does not support bridging if Exclusion is active.

SIP SBA for H.323 call

When an H.323 deskphone is active on a call, the SIP telephone displays the call as a simulated bridge appearance. The H.323 telephone can bridge onto the call by selecting the simulated bridge appearance. The system does not support bridging if Exclusion is active.

Call forward busy and Call coverage busy

A dual registered extension supports Call forward busy and Call coverage busy, regardless of which type of endpoint is busy.

Direct media

H.323 endpoint and SIP endpoint with a dual registered extension support direct media. Communication Manager uses initial direct media for a call involving a dual registered extension if all endpoints involved in the call are administered for Direct Media.

Mismatched number of buttons

The system lets the SIP and H.323 endpoints have a different number of buttons from each other. For example, the H.323 endpoint may support 24 buttons, but the SIP endpoint may be a conference phone that supports only a few buttons.

Automatic call back

You can activate automatic call back only from an H.323 endpoint. However, the feature works as expected on the dual registered extension.

Barge-in tone

The system supports this feature on a dual registered extension. If you set the **off-pbx-telephone configuration-set, Barge-in Tone** field to `y`, Communication Manager plays a tone when the other endpoint with the same extension number bridges onto an already active call.

Multiple calls and breaking in to a call

When a SIP endpoint and an H.323 endpoint with a dual registered extension are simultaneously active on independent calls, another endpoint can use one of the following features to break in to the call:

- Service observing
- Whisper page
- Intrusion
- Busy Verification

Limit Number of Concurrent Calls

The system supports the LNCC feature on dual registered endpoints. When you activate Limit Number of Concurrent Calls (LNCC) by using the FAC or by pressing the limit-call button on the H.323 deskphone, the LNCC feature limits the number of calls ringing at the extension even when the extension is using an OPTIM application.

Automatic hold

The system supports automatic hold on a dual registered extension.

Bridged appearance

SIP and H.323 endpoints with a dual registered extension can use multiline bridged appearance to originate, answer, and bridge on to calls to or from another telephone.

Busy-verify

SIP and H.323 endpoints with a dual registered extension support the Busy-verification feature.

Extend-call

SIP and H.323 endpoints with a dual registered extension can extend calls to other telephones.

Network failure

In a network connectivity failure, calls between SIP and H.323 phones with a dual registered extension remain active. Endpoints display bridge appearances after connection recovery.

Third Party Send All Calls

SIP and H.323 endpoints with a dual registered extension can send calls to a third party extension.

Third Party Enhanced Call Forwarding

SIP and H.323 endpoints registered with the same extension can forward incoming calls to different destinations depending on whether they are from internal or external sources.

Message Waiting Indicator (MWI)

H.323 and SIP endpoints support Message Waiting Indicator (MWI) for read and unread voice messages.

Multiple Device Access

Multiple Device Access (MDA) lets you register several SIP endpoints to the same extension. MDA is not supported together with Dual Registration, because a Dual Registration endpoint *must be* configured in System Manager using an H.323 endpoint type.

Chapter 161: SIP Calling Number Verification (STIR/SHAKEN)

Calling number verification is a SIP feature where the calling number is verified by the Internet Service Provider (ISP), and the results of that verification are included with the incoming call. The aim of this feature is to help reduce call spoofing.

- Support for and use of SIP calling number verification is mandated by law for US and Canadian locales. However, you can enable this feature in any locale if the local SIP ISP supports it.
- This feature only verifies the Calling number. The display name information supplied with calls is not verified.

ITSP looks at several factors to verify:

- Is the calling number associated with the subscriber making the call?
- Is the call coming from a known customer?
- Is the call originated by the known ITSP?
- Was the call digitally signed, and could the ITSP able to fetch the public certificate of the originating service provider to verify that the `SIP INVITE` had not been changed during transit?

The STIR/SHAKEN SIP Protocols

Internet Telephony Service Providers (ITSPs) implement the calling number verification using several SIP RFCs, collectively referred to as STIR/SHAKEN.

STIR

The Secure Telephony Identity Revisited (STIR) protocol uses digital certificates between the customer (the call originator) and the ITSP to establish customer authentication. The ISP can examine known numbers allocated to that customer for number authentication.

SHAKEN

Signature-based Handling of Asserted Information using toKENs (SHAKEN) are guidelines for PSTN network providers handling calls that transit from the non-SIP PSTN to SIP networks. Currently, it has mainly been implemented as a service for SS7 carriers in the USA and Canada.

For more information about STIR/SHAKEN SIP Protocols, see https://en.wikipedia.org/wiki/STIR/SHAKEN

SIP Calling Number Verification Display (STIR/SHAKEN)

After verifying the calling number, the authentic incoming calls will proceed with the regular call routing process. After the verification process is completed, the verified information will be displayed on the endpoints.

The customization is achieved by using the specific characters in the Code field of short codes or the Incoming Call Line Identification field of incoming call routes.

See the following table for the list of characters associated with the verification:

Character	Meaning	Description
V	Validation passed	It matches calls where the verstat value is set to `TN-Validation-Passed` plus the attestation level. If required, the level of attestation to match can be specified. Attestation levels are as follows: • `A` indicates Full Attestation. • `B` indicates Partial Attestation. • `C` indicates Gateway Attestation.
X	Validation failed	It matches calls that failed verification, meaning the call verstat value is set to `TN-Validation-Failed`.
?	No Validation	It matches calls that do not have any verification results or where the verstat value received is `NO-TN-Validation`.

The result of the verification process is then indicated in the call headers using a `verstat` value:

- `TN-Validation-Passed` plus an attestation level (see the table below). For example, `TN-Validation-Passed`.
- `TN-Validation-Failed` plus an attestation level (see the table below). For example, `TN-Validation-Failed`.
- `No-TN-Validation`

Attestation Level		Description
A	Full Attestation	The customer is known, and the calling number is associated with that customer. • When no authentication level is indicated or can be obtained, the IP Office treats the call as attestation level A.
B	Partial Attestation	The customer is known. However, the number is not associated with that customer. For example: • The customer is forwarding a call with an original calling number that is not associated with them. The call originates from another known ITSP, which is common for international calls.

Table continues…

Attestation Level		Description
C	Gateway Attestation	The call has come through a trusted source, but the original customer and number are unknown.

Chapter 162: SIP Dual Mode

With the SIP Dual Mode feature, the dual-mode device can use the EC500 feature or Wi-Fi to receive calls. The dual-mode device is a combination of a SIP wireless client and an EC500-enabled mobile phone.

Detailed description of SIP Dual Mode

When the dual-mode device is in the Wi-Fi range, the embedded dual-mode client registers remotely over SIP to Session Manager to receive calls. When the dual-mode device is not in the Wi-Fi range, the dual-mode device uses the EC500 feature to receive calls.

Note:

The Exclusion feature does not work on Avaya one-X® Communicator for Mac OS X phone in SIP Dual Mode.

From Communication Manager Release 6.3.6, this feature extends to CES users as well and is also known as EC500 Call Suppression. When a call is made to a SIP extension that uses a dual-mode mobile client and has a CES profile associated with it, the SIP extension receives two calls: a SIP call and a cellular call. The SIP extension shows an incoming SIP call for initial one to two seconds. Before the user accepts the call, the SIP extension receives a cellular call from Communication Manager. With the introduction of EC500 Call Suppression feature, the dual-mode client applications, such as Avaya Workplace Client for Android, receive only a single incoming call on the mobile phone for that particular extension. EC500 Call Suppression ensures that users receive an alert either by a VoIP call or a cellular call, but never both.

The following scenarios show the real-time application of EC500 Call Suppression. These scenarios require remote access.

- You are commuting and have configured the application to use the EC500 service. Also, you do not have Wi-Fi or cellular data access to Avaya Aura®. In this case, the EC500 service redirects all incoming calls on the deskphone to the mobile phone network.
- After you reach home, you can connect to the home Wi-Fi network and use the VoIP service. You continue to receive all incoming calls directed to the deskphone on the mobile phone by using the home Wi-Fi network over SIP. In this case, the server suppresses the EC500 cellular call to the mobile phone based on the use of VoIP.
- After you reach home, you can connect to the home Wi-Fi network and use the VoIP service. You continue to receive all incoming calls directed to the deskphone on the mobile phone

by using the home Wi-Fi network over SIP. In this case, the server suppresses the EC500 cellular call to the mobile phone based on the use of VoIP.

Limitation of SIP Dual Mode

When a call arrives on the dual-mode device soon after Communication Manager resets, you might receive two notifications of the call: one for EC500 and the other for SIP. You can answer the call on EC500 or SIP.

After the synchronization process with Communication Manager is complete, the dual-mode application does not display two incoming call notifications.

Screens for administering SIP Dual Mode

Screen Name	Purpose	Fields
Stations With Off-Pbx Telephone Integration	To add an OPS entry and EC500 entry on Communication Manager	• **Application** • **Phone Number** • **Trunk Selection** • **Config Set**

Administering SIP Dual Mode

Procedure

1. Through System Manager, create an extension of H.323 type.
2. On the SAT screen, type `change off-pbx-telephone station-mapping` *n*, where *n* is the extension that you added through SMGR.
3. On the Stations With Off-Pbx Telephone Integration screen, add an `OPS` application entry:
   a. In the **Application** field, type `OPS`.
   b. In the **Phone Number** field, type the station extension number
   c. In the **Trunk Selection** field, type TG, ars, aar, trunk group number, or ext, depending on the trunk group selection you want.
   d. In the **Config Set** field, type the configuration set number of the required call treatment options.
4. On the Stations With Off-Pbx Telephone Integration screen, add an `EC500` application entry:
   a. In the **Application** field, type `EC500`.

b. In the **Phone Number** field, type the cellular number

c. In the **Trunk Selection** field, type TG, ars, aar, trunk group number, or ext, depending on the trunk group selection you want.

d. In the **Config Set** field, type the configuration set number of the required call treatment options.

For more information on the Stations With Off-Pbx Telephone Integration screen, see *Avaya Aura® Communication Manager Screen Reference*.

5. Administer the Extend Call feature button through System Manager for the Dual Mode extension.

   See Administering the extnd-call feature button through System Manager.

Related links

Administering the extnd-call feature button through System Manager on page 780

Chapter 163: SIP digit handling

The Request URI in a SIP INVITE message, REFER message, or 3xx redirect response for INVITE message contains the following types of digits:

- Called-party digits
- Called-party and extra end-to-end digits

  For example, an authorization code or a voice mail password.

By default, Communication Manager assumes that the Request URI contains extra end-to-end digits, which might lead to incorrect call routing.

For example, a Request URI with 12 digits can match a Dial Plan entry of 7 digits. But Communication Manager processes the last 5 digits as extra digits. Similarly, for a SIP connection, if the Request URI does not contain extra digits, then the calls can be wrongly routed. The user can configure the Request URI as **called number-only** to avoid calls being wrongly routed.

With the SIP digit handling feature, you can configure Communication Manager to allow or restrict the extra end-to-end digits in the message.

Administration

Screens for administering Request URI Contents

Screen name	Purpose	Fields
PROTOCOL VARIATIONS **Note:** PROTOCOL VARIATIONS page is also part of the SIP trunk group form.	To configure Communication Manager to allow or reject the extra end-to-end digits in the SIP INVITE message, REFER message, or 3xx redirect response for INVITE message.	**Request URI Contents**

Setting up SIP digit handling

Procedure

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

   The system displays the Trunk Group screen.

2. On the PROTOCOL VARIATIONS screen, in the **Request URI Content** field, do one of the following:
   - Type **may-have-extra-digits**: Communication Manager routes an incoming Request URI without considering the total number of digits. Communication Manager might route the call using an entry that matches fewer digits than the total number in the Request URI.
   - Type **called number-only**: Communication Manager considers the total number of digits when routing an incoming Request URI. The routing fails if a match that incorporates all digits is unavailable.

     Note:

     The **called number-only** cannot be administered on Communication Manager that have variable length extensions.
3. Save the changes.

Interactions

Intercept treatment

If Communication Manager is non-authoritative, Communication Manager sends the INVITE with all digits back to Session Manager. Session Manager routes the call based on the authoritative domain. If Session Manager has routing administered for the digits, then the call routes accordingly. Else, Session Manager denies the call with 404 as No Route Found. The calling endpoint then plays a local failure tone. For example, an intercept tone.

Communication Manager does not receive an invalid number in an imsterm INVITE when Session Manager is configured correctly. Session Manager sends an INVITE to Communication Manager after validating the user number. Communication Manager treats the imsorig and imsterm cases consistently. missing period

Enbloc extensions

Communication Manager supports a special type of extension on the Dial Plan called an **enbloc extension**. You cannot dial the numbers of an **enbloc extension** from an endpoint keypad. To reach an **enbloc extension**, use a short code version or a prefixed version of the number.

Customers with E.164 numbering plans often assign the full E.164 numbers as enbloc extensions. Enbloc extensions prevent routing conflicts between the full E.164 numbers and the short code keypad dialing inside a branch. Enbloc extensions are reachable by an incoming SIP INVITE, which is an enbloc where all digits arrive at one time. Therefore, no digits follow regardless of how the Request URI parameter is set or whether the Request URI parameter supports extra end-to-end digits or not.

Chapter 164: SIP Direct Media

SIP Direct Media is supported by Communication Manager for Session Initiation Protocol (SIP) calls. SIP Direct Media signals the direct talk path between SIP endpoints before a call connects.

SIP Direct Media provides the following enhancements to SIP calls:

- Eliminates shuffling of SIP calls after call connects.
- Eliminates clipping on the talk path.
- Reduces the number of signaling messages for each SIP call.
- Reduces Communication Manager processing for each SIP call and increases the capacities of Communication Manager, Session Manager (SM), and SIP Busy Hour Call Completions (BHCC).
- Determines the media path early in the call flow and uses fewer media processor resources to configure the system.

Note:

When you originate a SIP call through Avaya Integral Enterprise Edition (formerly called Tenovis I55) and route the SIP call through Session Manager to Communication Manager, the system disables the SIP Direct Media feature. This results in a successful call.

Detailed description of SIP Direct Media

Using SIP Direct Media, the Communication Manager server acts as a tandem node and enables the endpoints to exchange media capabilities directly with each other. The system continues to monitor the codecs in the signaling messages and filters the calls based on the Call Admission Control and bandwidth constraints.

Second or subsequent forked calls can be EC500, Terminating Extension Group (TEG), or Coverage Answer Group (CAG).

Bridge call answer as Direct Media

Using the Bridge call answer as Direct Media feature, the calling party station can have direct media path with the bridge call appearance station of the called party station. The Bridge call answer as Direct Media feature is also known as the Bridge Direct Media feature.

For example, the calling party station is A, the called party station is B, and station B has a bridge call appearance on station C. If station A calls station B, and the call is answered by station C, then the call flow between station A and station C uses direct media.

Only 96x1 SIP endpoints support the Bridge call answer as Direct Media feature.

To enable the Bridge call answer as Direct Media feature, on page 19 of the FEATURE-RELATED SYSTEM PARAMETERS screen, set the **Allow Bridge DM Answer** field to y.

Call transfers

A user can keep any subsequent action on the second call, such as transfer, as direct media with the least occurrence of shuffling back to TDM resource. In case of consultative transfers, both the parties are directly on call if no **Music on hold** is applied and the call is shuffled in a single step. If **Music on hold** is ON, the held call is on TDM and the other call is direct media. When a telephone that is active on a call places the call on hold and the system does not have Music-on Hold configured, the hold operation is direct. In this case, Communication Manager transmits the SDP message received from the endpoint to indicate hold.

In case of unattended transfers, regardless of music on hold, the held segment of the call is on TDM to apply ring back and the other segment is direct.

Video forking

Communication Manager transmits all provisional responses with or without the SDP message received on each forked segment of the call to the call originator. Communication Manager supports multi-party audio conference with two-party video. The video is direct between the first two parties of the call, and the audio is mixed at Communication Manager.

Prerequisites enabling SIP Direct Media

- The call originator is SIP.

  If the call originator is not SIP, Communication Manager does not apply SIP Direct Media to the call.
- The following fields in the SIP signaling group screen of the originating SIP User Agent (UA) is set to y:
  - **Direct IP-IP Audio Connections**
  - **Initial IP-IP Direct Media**
- The call-originating party does not have a call on hold.
- If **Media Encryption Over IP** is y on the system-parameters customer-options screen (page 4), set **SDP Capability Negotiation for SRTP** to y on the system-parameters features screen (page 19).

Note:

If you do not meet with the prerequisites for SIP Direct Media, Communication Manager allocates media processors and shuffles the call after the connection is established.

SIP Direct Media enhancements

Using the SIP Direct Media feature, SIP endpoints establish a direct communication path for subsequent calls, Extension to Cellular (EC500) calls, 3PCC calls, forked video calls, and forked calls to multiple devices (MDA). The direct communication path is established before the call connects between the endpoints. Communication Manager uses the TDM resources or loops the media back to the Communication Manager server if required.

SIP to H.323 Direct Media

Communication Manager uses the SIP to H.323 Direct Media feature to directly connect SIP stations or SIP trunks to H.323 stations, without using a media resource and shuffling the call.

When a call connects, the Direct Media feature signals a direct talk path from a SIP station or a SIP trunk to an H.323 station. The Direct Media feature can be activated on the Signaling Group screen, in the **Initial IP-IP Direct Media** field. To establish a direct path during a call setup, SIP stations and H.323 stations must use the same IP version, IPv4 or IPv6.

The benefits of using the SIP to H.323 Direct Media feature are:

- Elimination of the SIP to H.323 call shuffling after the call connects
- Elimination of clipping on the talk path
- Decrease in the number of signaling messages for each SIP to H.323 call
- Early detection of the media path in the call flow and use of fewer media processor resources to configure the system
- Reduction in the processing time of each SIP-H.323 call, and increase in the SIP Busy Hour Call Completions (BHCC) capacity

For more information on the **Initial IP-IP Direct Media** field, see *Avaya Aura® Communication Manager Screen Reference*.

Chapter 165: SIP SRTP enhancements

In the offer/answer model, Session Description Protocol (SDP) does not have a defined capability to negotiate one or more alternative transport protocols or attributes. For example, in the offer/answer model, SDP does not have a defined capability to negotiate the Real-time Transport Protocol (RTP) profiles. This SDP behavior has the following capability limitations:

- deployment of new RTP profiles, such as Secure Real-time Transport Protocol (SRTP), or RTP, or Real-Time Transport Control Protocol (RTCP)-based feedback
- negotiate use of different security keying mechanisms

To overcome the SDP limitations, the SDP capability negotiation feature implements a set of potential configurations indicating which combinations of capabilities and associated media components can be used for negotiating a session. During a session, the negotiation process implements the potential configurations as the input and provides the negotiated actual configurations as the output.

Note:

The SDP capability negotiation feature also supports SIP Direct Media. However, the SDP capability negotiation feature is not required because of SIP Direct Media.

You can implement the SDP capability negotiation feature to support SIP Direct Media and enhance the SIP SRTP capability in Avaya Aura® Communication Manager.

SIP SRTP enhancements in Communication Manager supporting SDP capability negotiation cause some memory overhead on the system. However, the memory overhead is insignificant and does not involve any bandwidth overhead.

Detailed description of SIP SRTP enhancements

Communication Manager supports and enhances the SIP SRTP capability by using SDP capability negotiation. SDP Capability Negotiation is a mechanism that enables SDP to provide limited support to indicate system capabilities and the associated potential configurations and negotiate the use of the potential configurations as actual configurations. SDP Capability Negotiation provides a general SDP Capability Negotiation framework that is backward compatible with the existing SDP and defines specifically how to provide attributes and transport protocols as capabilities and negotiates them using the framework. The SIP SRTP enhancements in Communication Manager enable the following:

- Support the SIP User Agent (UA) to provide both SRTP and non-SRTP capabilities in a single SDP Capability Negotiation.

- Support Direct Media functionality in Communication Manager by eliminating the requirement of NULL INVITE at the Callee leg during the initial call setup.
- Simplify the SIP SRTP call flow.
- Enable the SIP endpoints and Communication Manager to provide complete encryption capabilities to each other and increases the call shuffling capability of Communication Manager.

SIP signaling with SDP capability negotiation is backward compatible with the existing SRTP implementation and also with SIP implementations not supporting SRTP.

Note:

SIP SRTP enhancements in Communication Manager using SDP capability negotiation require changes only in the SIP signaling implementation. The SRTP media path does not undergo any change to implement SDP capability negotiation.

Communication Manager behavior with SRTP Capability Negotiation

If SRTP Capability Negotiation is enabled, the capability negotiation call flow is as follows:

- Communication Manager sends out INVITE with SDP Capability Negotiation.
- Communication Manager accepts incoming INVITE with SDP Capability Negotiation.

If SRTP Capability Negotiation is disabled, the capability negotiation call flow is as follows:

- Communication Manager sends out INVITE with null SDP on the Callee leg and negotiates based on the SRTP or RTP returned from remote. In case of SRTP, Communication Manager follows the SDES SRTP grammar.
- Communication Manager does not accept any SDP capability proposed in the capability negotiation format. For example, if RTP is proposed in the regular SDP format and SRTP is proposed in the capability negotiation format, Communication Manager considers it as RTP. However, if SRTP is proposed in the regular SDP format and RTP is proposed in the capability negotiation format, Communication Manager considers it as SRTP.

Chapter 166: SIP Agent Reachability

The SIP Agent Reachability feature determines the availability of a SIP station. The SIP station acts as an agent for both Communication Manager and AES applications.

Session Manager maintains the registration state of a SIP station. However, the station might not be reachable from Communication Manager because of a network outage between the station and Session Manager or Avaya SBC, or a disruption between Communication Manager and Session Manager.

After you enable the SIP Agent Reachability feature, Communication Manager can detect the reachability status of a SIP station and take actions as configured.

Detailed description of SIP Agent Reachability

The SIP Agent Reachability feature determines the availability of a SIP station. The SIP station acts as an agent for both Communication Manager and AES applications.

Session Manager maintains the registration state of a SIP station. However, the station might not be reachable from Communication Manager because of a network outage between the station and Session Manager or Avaya SBC, or a disruption between Communication Manager and Session Manager.

After you enable the SIP Agent Reachability feature, Communication Manager can detect the reachability status of a SIP station and takes actions as configured.

The feature works as follows:

Communication Manager checks the reachability status of idle agents and idle domain controlled SIP stations, if enabled by configuration. The frequency of the attempts is determined by the SIP **Reachability Polling Interval** field on the system-parameters-features form.

When a SIP station is unavailable, Communication Manager does the following:

- SIP agent: When the first reachability attempt fails, Communication Manager puts the agent in the aux-work mode with the ROOF reason code. If the agent is already in aux-work mode with ROOF reason code, the agent decreases the reachability attempts, as administered in **SIP Station Reachability Attempts** by one. If the agent is already in aux-work mode, however with a different reason code, the agent is removed to aux-work with ROOF reason code.
- Domain controlled station: Communication Manager should update the application by sending the Registered out-of-service message.

To differentiate between a temporary network disruption and a network outage, Communication Manager continues to make attempts in determining the reachability status of the stations. The number of additional attempts is determined by the value configured in the **SIP Station Reachability Attempts** field on the system-parameters-features form. If the station becomes reachable in any of the attempts, Communication Manager takes appropriate actions as follows:

- SIP agent: The agent continues to remain in the aux-work mode. The station used by the agent is notified that it is in the aux-work mode.
- Domain controlled station: No operation.

If all the attempts fail, Communication Manager declares the station unreachable and does the following:

- SIP agent: Communication Manager logs out the agent with the reason code configured on Forced Agent Logout for Unreachable Reason Code on the system-parameters-feature form.
- Domain controlled station: Communication Manager should update the application with Unregistered out-of-service message.

After the station is unreachable, Communication Manager continues to determine the reachability status of a station for the duration as configured in the **SIP Unreachable Polling Period** field on the system-parameters-features form. If Communication Manager determines that a station is reachable during the period, Communication Manager does the following:

- SIP agent: Update the status of the station with the agent's logged-off state.
- Domain controlled SIP station: Communication Manager should update the Application with Unregistered out-of-service message.

Otherwise, after the duration is over, Communication Manager does the following:

- SIP agent: Communication Manager stops determining the reachability status of the station.
- Domain controlled SIP station: Communication Manager stops determining the reachability status of the station. Communication Manager resumes the action when the station logs in again.

Limitations of SIP Agent Reachability

The SIP Agent Reachability feature has the following limitations:

- SIP Agent Reachability feature is network-intensive and is a CPU.
- Receives a lower priority than call processing and other competing services on Communication Manager. Therefore the feature can take a longer duration to determine the reachability of the stations in the period as administered in the **SIP Reachability Polling Interval** and **SIP Unreachable Polling Period** fields.
- Starts 15 minutes after the specific Communication Manager is started.
- Determines the reachability status of a SIP Station by polling the respective Session Manager designated for the SIP station. Communication Manager determines the designated Session Manager by determining the route-pattern. Therefore a trunk-group is required to reach Session Manager.

- Does not consume any trunk resources.
- Reachability determination using the SIP OPTIONS message does not interact with Look Ahead Routing (LAR). If OPTIONS polling fails with the primary Session Manager, the polling is retried with the secondary Session Manager(if administered) irrespective of LAR administration.

Administering SIP Agent Reachability

Procedure

1. Type change system-parameters features. Press **Enter**.
2. On the FEATURE-RELATED SYSTEM PARAMETERS screen, in the **SIP station reachability checking options**, set the **Enable SIP Agent Reachability** field to one of the following options:
   - To enable the polling feature for all SIP agents, type `y`.
   - To disable the polling feature for all SIP agents, type `n`.

   Note:

   The default option is set to `n`.
3. Set the **Enable reachability for station domain control** to one of the following options:
   - To enable the polling feature for all Domain controlled SIP stations that have the reachability option set to `system` on the station configuration page, type `y`.
   - To disable the polling feature for all Domain controlled SIP stations that have the reachability option set to `system` on the station configuration page, type `n`.
   - To disable the polling feature for all Domain controlled SIP stations irrespective of the option selected on the station form, type `disable all`.

   Note:

   The default option is set to `n`.

Enabling and disabling reachability per domain controlled stations

Procedure

1. Type change station <extension> for a SIP station type. Press **Enter**.

2. On the Stations screen, in the SIP Feature Options, set **Enable Reachability for Station Domain Control? [System/Y/N]** field to one of the following options:
   - To enable the polling feature, type `y`.
   - To disable the polling feature, type `n`.
   - To take action based on the option selected on the system-parameters features form, type `system`.

   Note:

   The default option is set to `system`. The administration option has effect only if the station is domain-controlled.

   When the system-parameters features form is set to `disable-all`, the **station form** field is overridden or made inaccessible.

Chapter 167: SIP trunk optimization

Overview

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. The following illustration explains the problem of trunk consumption due to redundancy.

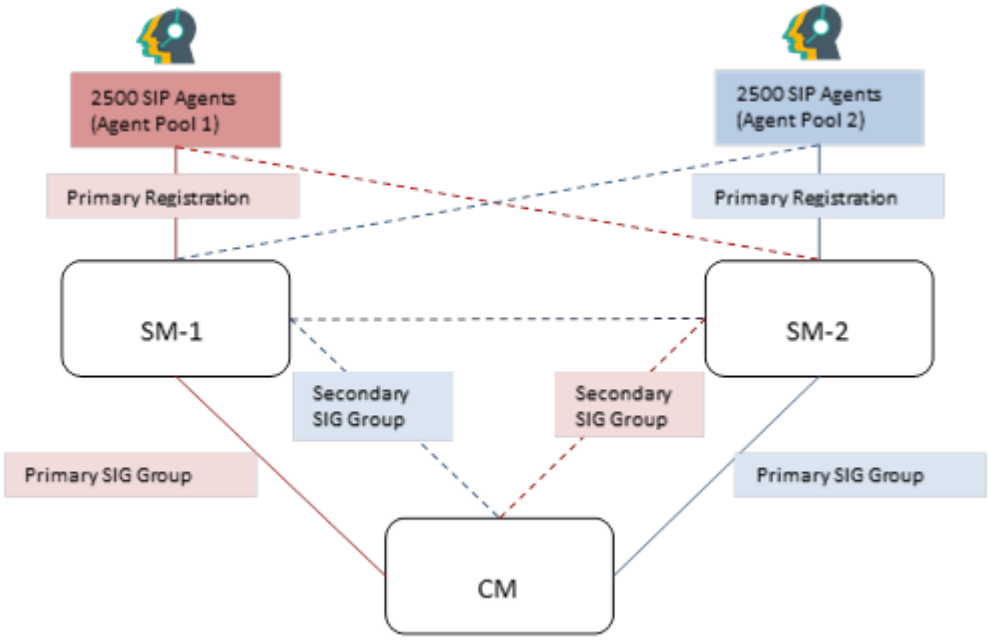


Figure 31: Scenario 1 of trunk consumption due to redundancy

The above figure provides the following 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, if Session Manager- 1 and Communication Manager connection is broken, or if Session Manager-1 fails, then Communication Manager has an alternate path to reach the red agents through Session Manager-2 using the blue trunk. With 2500 trunk members between Communication Manager and Session Manager-2, 5000 agents from both the agent pools cannot be supported. Same is the case if the blue agents fail over to Session Manager-1.

To address the issue on the second scenario, additional trunks must be administered between Communication Manager and Session Manager-1 and also between Communication Manager and Session Manager-2. To support failover of 2500 red agents over to Session Manager-2, additional 2,500 trunk members must be administered between Communication Manager and Session Manager-2. Similarly, to support failover of blue agents over to Session Manager-1, additional 2,500 trunk members must be administered between Communication Manager and Session Manager-1. To support the second scenario, additional trunks are shown by the dotted lines in the following figure.

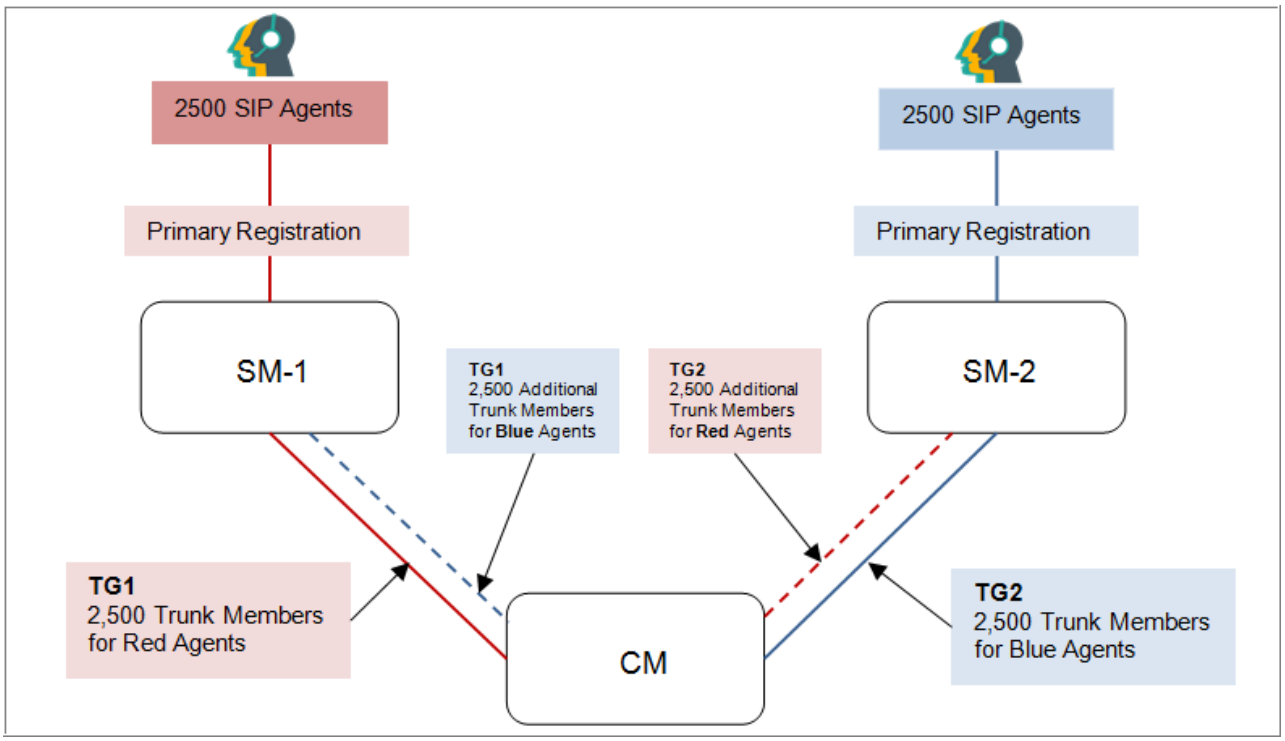


Figure 32: Scenario 2 of trunk consumption due to redundancy

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.

Note:

When the policy-based assignment is enabled in System Manager, you can administer up to four Session Managers for a SIP station.

- Double the number of trunks must 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 become 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 enables 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 28 Session Managers. With a Session Manager cluster, it is assumed that all Session Managers share a similar configuration, and any Session Manager can route a call to the far end station or far-end trunk.

The ability of the signaling group to point to both Session Managers reduces the required trunks to be administered on Communication Manager by half while achieving full redundancy. If the link to Session Manager-1 fails, the Signaling group uses the link to Session Manager-2 to route all the outgoing traffic. The effect of 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 deliver traffic.
- For example, a trunk group with 5000 members in the first scenario can service 2500 agents on Session Manager-1 and 2500 agents on Session Manager-2. If the connectivity between Communication Manager and Session Manager-1 goes down, the same trunk group with 5000 members can service 2500 agents on Session Manager-1 and 2500 agents on Session Manager-1 and 2500 agents on Session Manager-2 through the link between Communication Manager and Session Manager-2. Even if Session Manager-1 goes down and all agents move to Session Manager-2, the same 5000 members can reach all the 5000 agents.

The SIP trunk optimization feature are as follows:

- Number of trunk members is 9,999 for SIP trunk groups.

- Number of SIP agents is 10,000.
- System-wide trunk members is 30,000.
- Measured trunks is 30,000.
- TLS connections for SIP is 56 from 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 information about the capacities, see *Avaya Aura® Communication Manager System Capacities Table*.

  Note:

  When the policy-based assignment is enabled in System Manager, you can administer up to four Session Managers for a SIP station.
- Look Ahead Routing feature is deprecated for SIP station calls if routed over clustered signaling group.
- Route pattern can now specify a network region.

Screens for administering SIP trunk optimization

Screen name	Purpose	Fields
Cluster Session Manager	Allows you to administer up to 10 clusters of Session Manager. Cluster Number is a read-only field.	Cluster Number Cluster Name Session Manager node names
Signaling Group	Allows you to administer a Cluster ID if the Clustered field is set to `y`. Administration of a Session Manager cluster on a Signaling Group form allows the signaling group to point to all Session Managers in the cluster. The Peer Server and Enable Layer 3 Test fields are read-only if the Clustered field is set to `y`. If the Clustered field is set to `n`, you can edit the Peer Server and Enable Layer 3 Test fields.	Clustered Cluster ID Peer Server Enable Layer 3 Test

Table continues…

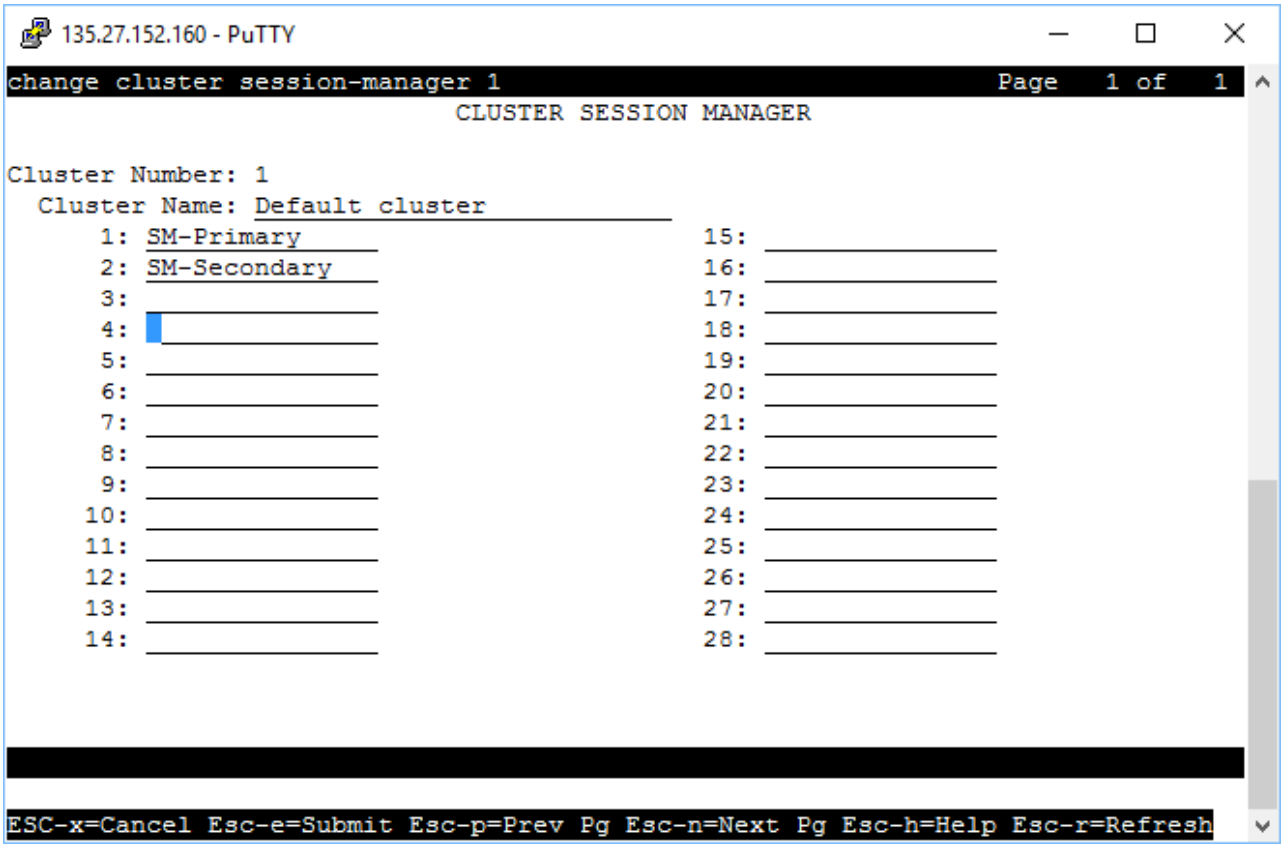
Screen name	Purpose	Fields
Station	Displays the primary, secondary, third, and fourth Session Managers to which the SIP Trunk Optimization feature sends the Invite to the station. Primary, secondary, third, and fourth Session Manager fields are read-only on the SAT interface. They are populated by System Manager during SIP station administration or translation synchronization between System Manager and Communication Manager in case of already administered SIP stations. IP addresses are allocated to these fields only when the policy-based assignment is enabled in System Manager.	Primary Session Manager Secondary Session Manager Third Session Manager Fourth Session Manager
Trunk Group	Allows you to configure the number of trunk members that can be administered on a SIP trunk group.	Number of Members
Route Pattern	Displays the network region for each of the route preference on the route patterns.	Network Region
IP Options System Parameters	If the signaling group is clustered, you see the following options: • Primary Session Manager Bandwidth Manager • Secondary Session Manager Bandwidth Manager	Node-Name of Primary SM BW Mgr Node-Name of Secondary SM BW Mgr

Cluster Session Manager

Use this screen to administer Session Managers. You can administer up to 10 clusters of Session Managers by using the Communication Manager CLI. The node names administered on this screen can be either of IPv4 or IPv6 address. For example, if the primary Session Manager points to an IPv4 type address, then the secondary Session Manager must be IPv4 address type. The node names cannot be a mix of IPv4 and IPv6 address types on the same cluster.

To administer cluster Session Manager screen, use the following command:

```
change cluster session-manager
```



Cluster Number

By default, there are 10 clusters.

Cluster Name

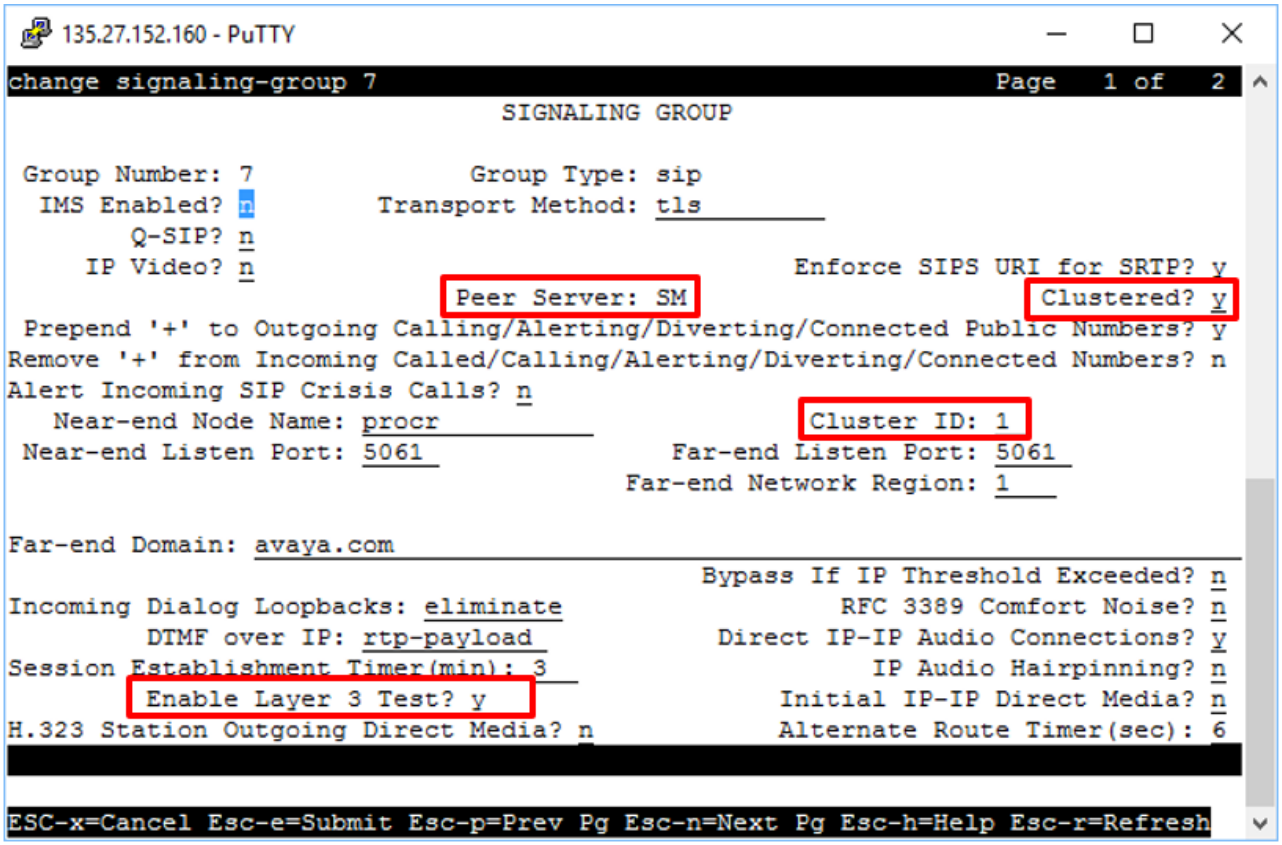
Use this field to add Session Manager node names.

Signaling group

The signaling group allows for administration of a “Cluster ID”, if the **Clustered** field is set to ‘y’. Cluster ID is a new field that allows for association of a Session Manager cluster with a signaling group. The field “Far-end Node Name” will be replaced with field “Cluster ID” up on setting “Clustered” to ‘y’. The “Peer Server” field will be read only and will be set to `SM`. The **Enable Layer 3 Test** field will be set to `y` and will be read only. The clustering functionality works only with Avaya Aura® Session Manager.

Administration of a Session Manager cluster on a Signaling Group form allows the signaling group to point to all Session Managers in the cluster. In this example, see the figure in the Cluster Session Manager section and figure in the Signaling group section, the signaling group is pointing to primary and secondary Session Managers.

The SIP signaling group remains in service if at least one Session Manager is reachable from Communication Manager. The signaling group is out of service if all the Session Managers in the cluster are not reachable.



Station

In the Station form, the SIP Station type has the following fields; **Primary Session Manager**, **Secondary Session Manager**, **Third Session Manager**, and **Fourth Session Manager**. These fields are populated from System Manager and are read-only on the Communication Manager SAT interface. These fields cannot be modified on the Communication Manager SAT interface. If the call to this SIP station is routed to a SIP trunk (via AAR/ARS and then route pattern or trunk group) that has a clustered signaling group, then SIP Trunk Optimization feature sends the Invite for the station to SM-Primary. If SM-Primary is not reachable, then the Invite is sent to SM-Secondary. The Session Manager selection for routing to a SIP station does not apply to a call between two SIP stations. In this case, the Session Manager itself decides the destination Session Manager for the called SIP station.

IP addresses are allocated to these fields only when the policy-based assignment is enabled in System Manager.

```
display station 31100000                                    Page   6 of   6
                                    STATION
SIP FEATURE OPTIONS

     Type of 3PCC Enabled: None     SIP Trunk: aar
 Enable Reachability for Station Domain Control: s
SIP URI:
Primary Session Manager
  IPv4 Address: 10.133.57.130      IPv6 Address:
IPv4 Node Name: sm                 IPv6 Node Name:

Secondary Session Manager
  IPv4 Address:                    IPv6 Address:
IPv4 Node Name:                    IPv6 Node Name:

Third Session Manager
  IPv4 Address:                    IPv6 Address:
IPv4 Node Name:                    IPv6 Node Name:

Fourth Session Manager
  IPv4 Address:                    IPv6 Address:
IPv4 Node Name:                    IPv6 Node Name:
```

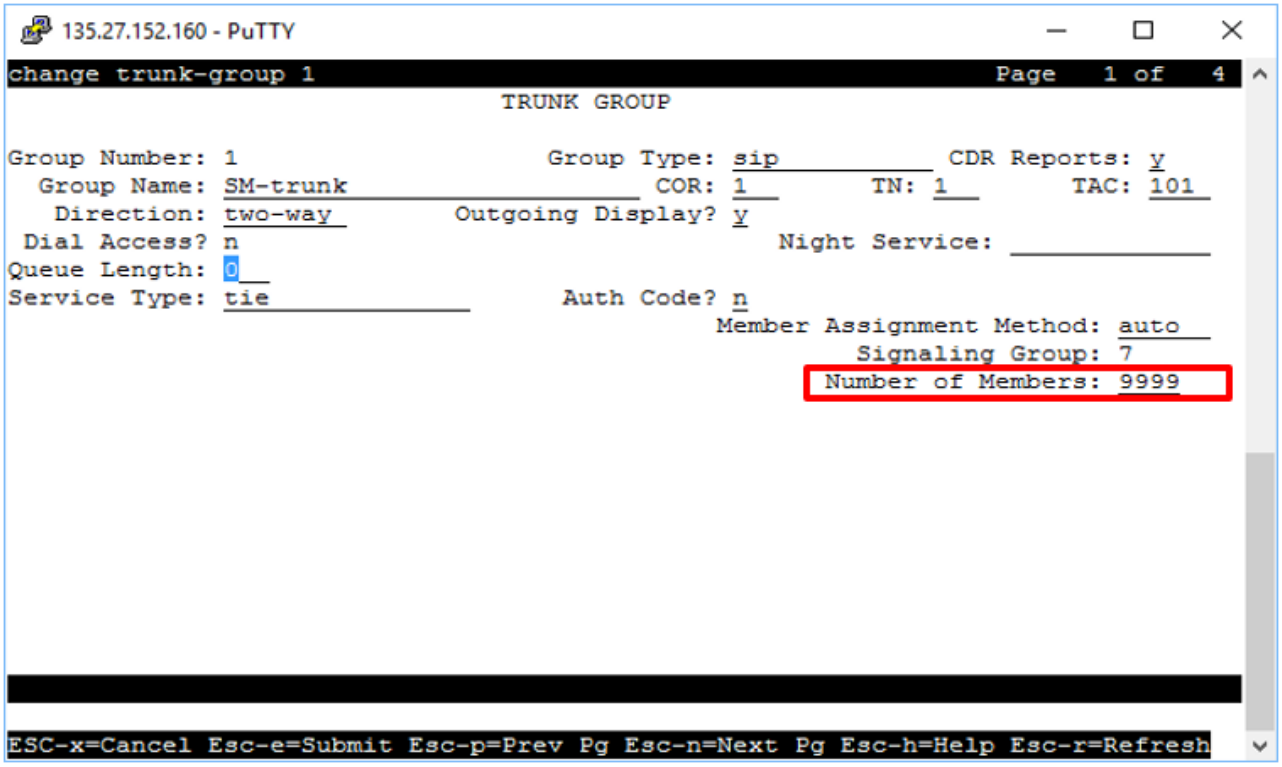
Trunk group

In Communication Manager, the number of trunk members that can be administered on a SIP trunk group is increased to 9,999 from a current value of 255. This allows for fewer trunk groups to be administered on a route pattern. More than 255 trunk members can be administered if Member Assignment field is set to ‘auto’. Pages for members are not shown on a SIP trunk group form. Only 1500 members can be added or removed simultaneously on a trunk group.

The following are applicable for Trunk calls and not to SIP station calls:

- **Network Region** field on the Route Pattern screen applies only for trunk and OPTIM such as EC500 and telecommuter calls but not for SIP station calls.
- This overrides the **Network Region** field on the SIP signaling group for the above-mentioned applicable calls.

Session Manager from the SIP cluster is selected in a round-robin fashion to route the call. It is assumed that any Session Manager on the cluster can route the call to the intended far-end. On receiving a LAR triggering response, another Session Manager from the cluster is selected to route the call. Up to 5 attempts (to unique Session Managers) are made to route the call using the same trunk group and member. On failure of all 5 attempts, the next entry in the route pattern can be used to route the call if LAR is enabled.



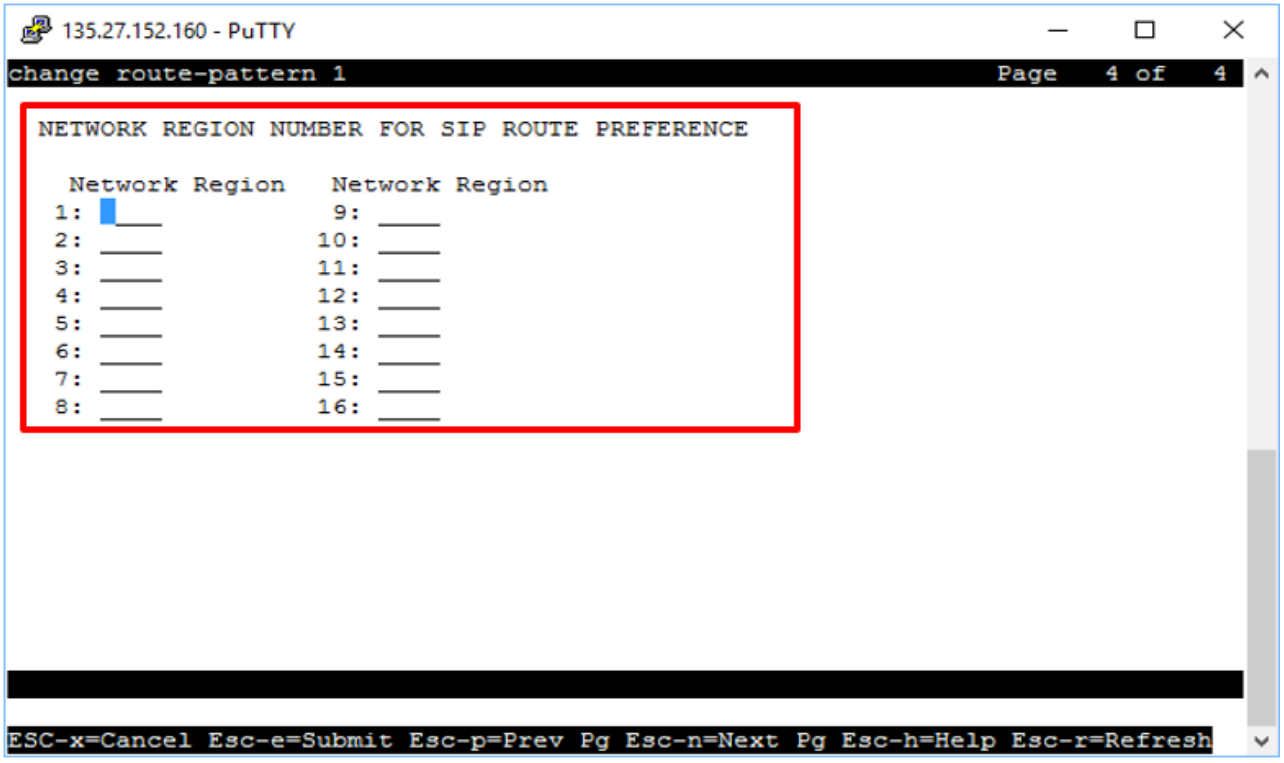
Route pattern

A network region can be populated for each of the route patterns. This network region will be used only when routing SIP trunk calls (SRE Calls) over the route preference (Trunk Group).

Network region field on the route pattern applies only for trunk and OPTIM such as EC500 and telecommuter calls but not for SIP station calls. This overrides the network region field on the SIP signaling group for the above mentioned applicable calls.

Route patterns are as follows:

- Routing to SIP stations using a non-clustered signaling group
- Routing to SIP stations using a clustered signaling group
- Routing to SIP trunk calls using clustered signaling groups



Route pattern to SIP stations using a non-clustered signaling group

- If the SIP trunk group does not use a clustered signaling group, the Session Manager fields on the SIP station form are not used to route to the SIP station.
- Two trunk groups and two trunk members are required to reach the SIP station. One to the Primary Session Manager and other to the Secondary Session Manager in a fully redundant configuration.
- If the Primary Session Manager is not reachable, another trunk group must be selected from the Route Pattern that routes to the Secondary Session Manager using Look Ahead Routing (LAR). For non-clustered signaling group, LAR can be used for both SIP station calls and trunk calls.
- This is pre-Communication Manager 8.0 functionality and can be used in Communication Manager 8.0 and later.
- The newer SIP routing functionality using a clustered signaling group is optional and can be used if needed, but not forced.

Route pattern to SIP stations using a clustered signaling group

- All Session Managers used by all SIP stations on a Communication Manager should be administered on the SIP cluster. Trunk groups should use clustered signaling groups.
- The Primary Session Manager to route to the station is selected from the SIP station form. As the clustered signaling group can send a message to any Session Manager in the cluster, the call can be sent to the Primary Session Manager using that trunk group.
- In case of a failover scenario when the Primary Session Manager is not reachable, the secondary Session Manager to reach to the SIP station is taken from the SIP station form.

The call is sent using the same trunk group and trunk member. A different trunk group (and signaling group) is not needed.

- There is no need of Look Ahead Routing (LAR) because the same trunk group and trunk member can be used to route to both Session Managers. Hence, LAR is not applicable if clustered signaling groups are used to route to SIP stations.

Route pattern to SIP trunk calls using clustered signaling groups

- Session Manager from the SIP cluster is selected in a round robin fashion to route the call.
- It is assumed that any Session Manager on the cluster can route the call to the intended far-end.
- On receiving a LAR triggering response, another Session Manager from the cluster is selected to route the call. Up to five attempts (to unique Session Managers) will be done to route the call using the same trunk group and member.
- If all the five attempts are failed, the next entry in the route pattern can be used to route the call if LAR is enabled.

IP-options system parameters

IP Bandwidth Management page displays the primary Session Manager bandwidth manager and secondary Session Manager bandwidth manager nodes, when a clustered signaling group is administered.

Each Communication Manager can have only two Session Managers to manage bandwidth, if centralized Session Manager managed bandwidth is being used. Administration of one clustered signaling group is sufficient to push bandwidth notification to both bandwidth management Session Managers.

Best practices

Use the following best practices for SIP trunk optimization:

- A mix of clustered and non-clustered signaling group should not be administered for the same set of Session Manager and having the same port.
- If an implementation must have multiple signaling group with the same Session Manager that are mix of clustered and non-clustered, then the port must be different.
- All Session Managers that are administered in the cluster Session Manager form must have entity links administered between them in a star topology.
- All Session Managers that are administered in the cluster Session Manager form must have Session Manager Release 8.0 or higher for SIP trunk optimization feature to work correctly.
- Session Manager auto suggest feature that is administered on the route pattern form is deprecated with clustered signaling groups.
- Primary Session Manager and secondary Session Manager associated with a station must be administered on the cluster.

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.

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.

Chapter 168: SIP undelivered call notification

The SIP undelivered call notification feature provides a notification about the undelivered call to the endpoint. The endpoint logs this entry in the missed call log.

Communication Manager enables the undelivered call notification and sends the notification to Session Manager. Session Manager forwards the notification to the endpoint, and the endpoint logs the entry in the missed call log.

This feature has the following requirements:

- Communication Manager Release 6.3.6 or later
- Session Manager Release 6.3.8 or later
- 96x1 SIP endpoints Release 6.4 and later or Avaya one-X® Communicator for Windows SIP endpoints Release 6.2 or later.

This feature does not require any administration on Communication Manager or Session Manager and is available to the users by default. However, the **Enable Layer 3 test** field must be set to `y` on the signaling group between Communication Manager and Session Manager so that Communication Manager can understand the capabilities of Session Manager.

Communication Manager sends the undelivered call notification when a call is made directly to an endpoint but is not delivered to it. The following features trigger this notification:

- All call appearances are busy.
- Limit Number of Concurrent Call is activated and the endpoint is busy.
- Call Forward Busy or Call Forward All is enabled.
- Enhanced Call Forward (ECF) unconditional or ECF busy is enabled.
- Cover All Calls is enabled.

Related links

Interactions for SIP no Call Appearance missed call logging on page 1273

Interactions for SIP no Call Appearance missed call logging

Offline Call Journaling

In the Offline Call Journaling feature, Session Manager tracks the incoming, outgoing, and missed calls to the endpoint. When the endpoint is logged out, the SIP no Call Appearance missed call logging feature works with the offline call log.

Bridged Call Appearance

If the primary endpoint missed a call, only the primary endpoint receives the undelivered call notification. The bridged appearances do not receive the notification.

Multi-Device Access

If a call is not delivered to the extension, Session Manager sends the undelivered call notification only to the SIP telephones that are capable of receiving the notification.

Dual Registration

If a call is not delivered to the extension, Communication Manager and Session Manager send the undelivered call notification to the H.323 and SIP endpoints respectively, if the endpoint is capable of receiving the notification.

SIP agent and Call Center Elite

Agent extensions do not support SIP no Call Appearance missed call logging.

Hunt group

Hunt group do not support SIP no Call Appearance missed call logging.

1xC SIP in shared control mode

The Avaya one-X® Communicator for Windows SIP endpoints in the shared control mode support the SIP no Call Appearance missed call logging feature.

ASAI notification

An undelivered call triggers both SIP no Call Appearance missed call logging as well as ASAI undelivered call notification.

Related links

SIP undelivered call notification on page 1272

Chapter 169: SIP Resiliency

When the SIP signaling path for a call between user agents is disconnected due to SIP element failure or the network unavailability, the user agents cannot exchange the signaling messages. The SIP signaling path can also be disconnected when one or more SIP elements such as proxy or location server are not working, if the user switches the network from WiFi to 4G and from 4G to Wifi, or the failure of Session Manager.

Using SIP Resiliency feature, Session Manager reconstructs the call between endpoints when the SIP signaling path for a call or a conference call is disconnected. Avaya recommends using same domain names for signaling groups to support call reconstruction.

Session Manager reconstructs the impacted SIP dialog by initiating a new dialog towards SIP user agents to replace the dialog of broken end to end call. In case of Session Manager failure, alternate Session Manager reconstructs the call.

Communication Manager supports SIP Resiliency feature by replacing SIP dialogs for each dialog of a SIP session. When Communication Manager receives INVITE request containing a Replaces header message, Communication Manager attempts to replace the SIP dialog specified in the Replaces header. The Communication Manager also maintains the integrity of a call so that the features such as hold or transfer during the call are available for the parties of the call.

For the best performance of call reconstruction, ensure that the administration settings on the signaling groups, trunk groups, network regions, and codec settings are uniform between primary Session Manager, alternate Session Manager, and Communication Manager that are configured for call reconstruction. Also, ensure that all the incoming SIP trunks must connected to Communication Manager through Session Manager.

The call reconstruction might fail if the call topology consists of old as well as new instances of Session Manager and Communication Manager.

SIP device must also support the new call reconstruction method for SIP Resiliency feature to work.

You can enable SIP Resiliency only if all the Session Managers in the configuration are 8.0 or later.

For more information on Communication Manager settings for SIP Resiliency, see *Avaya Aura® Communication Manager Screen Reference*.

Related links

Enabling SIP Resiliency on page 1275

Enabling SIP Resiliency

About this task

Use this procedure to enable SIP resiliency for call reconstruction.

Procedure

1. On the home page of System Manager web console, in **Elements**, click **Session Manager** > **Global Settings**.
2. Select the **Enable SIP Resiliency** check box.
3. Click **Commit**.

Related links

SIP Resiliency on page 1274

Chapter 170: Source-based Routing

Communication Manager uses the Source-based Routing feature to send the location information of H.323, DCP, and analog stations to Session Manager.

Related links

Detailed description of Source-based Routing on page 1276
Screen for administering Source-based Routing on page 1276
Administering Source-based Routing on page 1277

Detailed description of Source-based Routing

Communication Manager includes the IP address of the caller in the bottom-most Via header of the Invite message and transmits the message to Session Manager. Session Manager uses the IP address to select the matching trunk or route pattern and then routes the call to destination stations.

Related links

Source-based Routing on page 1276

Screen for administering Source-based Routing

Screen	Purpose	Fields
Trunk group protocol variations	Configure Communication Manager to send the location information of H.323, DCP, and analog stations to Session Manager.	Block sending Calling Party Location in INVITE

Related links

Source-based Routing on page 1276

Administering Source-based Routing

Before you begin

On the Trunk Group screen, ensure that the value of the **Group Type** field is *sip*.

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.

Related links

Source-based Routing on page 1276

Chapter 171: Station Hunting

Use the Station Hunting feature to find an extension that is available to answer a call when the called extension is busy. The system checks for an idle extension in the station-hunting chain of the called extension before the system routes the call to the coverage path of the called extension.

The Station Hunting feature supports the following capabilities:

Station Hunting Before Coverage

If the system finds an idle extension in the station-hunting chain of the called extension, the system leaves the call at the idle extension.

Station Hunting After Coverage

If the system does not find an idle extension in the station-hunting chain of the called extension, the system routes the call to the coverage path of the last extension in the station-hunting chain.

Detailed description of Station Hunting

To use Station Hunting, you create a station-hunting chain. This chain governs the order in which the system routes the calls when the system encounters a busy station. Each station in the chain links to only one subsequent station in the station-hunting chain. However, a station can be the receiving link from any number of station-hunting chains.

When the system starts to check the station-hunting chain, the system updates the display of the calling party with an h. The system also updates the display of the called party with an h.

You can administer an unlimited number of extensions in a station-hunting chain.

The table on page 1278 shows how the system routes a call through the station-hunting chain.

Table 88: Routing calls through a Station Hunting chain

Condition	Response
The extension is idle.	• The caller hears ringing. • The system discontinues to route the call through the station-hunting chain.
The extension is busy.	The system routes the call to the next extension in the station-hunting chain.

Table continues…

Condition	Response
The **hunt-to-station** field on the Station screen of the extension is blank.	• The caller hears busy tone. • The system discontinues to route the call through the station-hunting chain.
The system encounters a station in the station-hunting chain for the second time.	• The caller hears busy tone. • The system discontinues to route the call through the station-hunting chain.
The system checks 30 extensions in the station-hunting chain, and does not find an idle extension.	• The caller hears busy tone. • The system discontinues to route the call through the station-hunting chain.

Station Hunting and Call Coverage

You can administer the system to perform station hunting before the system sends calls to coverage, or after the system sends calls to coverage.

If you administer the system to use Station Hunting before the system uses Call Coverage, the system checks for a hunt-to station at the called extension. If the system finds a hunt-to station at the called extension, the system routes the call down the station-hunting chain. If the system does not find an idle extension in the station-hunting chain, the system routes the call to coverage.

Station Hunt chain station removal

When you remove a station from a station-hunting chain, the system attempts to maintain the chain. Consider the following examples:

- Station 1 links to station 2, and station 2 links to station 3. If you remove station 2, the system links station 1 to station 3.
- Station 1 links to station 2. Station 2 does not link to another extension. If you remove station 2, station 1 no longer links to another extension.

Station Hunt chain station duplication

When you duplicate a station, the system does not copy the extension that is in the **hunt-to station** field on the Station screen to the station that you duplicate.

Station Hunting administration

The following tasks are part of the administration process for the Station Hunting feature:

- Assigning station hunting after coverage
- Assigning a hunt-to station to an extension
- Administering Station Hunting before Coverage

Related links

Assigning station hunting after coverage on page 1280
Assigning a hunt-to station to an extension on page 1280
Administering Station Hunting before Coverage on page 1281

Screens for administering Station Hunting

Screen name	Purpose	Fields
Coverage Path	Activate the Hunt after Coverage capability for a coverage path.	Hunt After Coverage
Station	Assign a hunt-to station to an extension.	Hunt-to Station
System-Parameters Call Coverage/ Call Forwarding	Enable the Station Hunting before Coverage capability for your system.	Station Hunt Before Coverage

Assigning station hunting after coverage

Procedure

1. Enter `change coverage-path n`, where *n* is the number of the coverage path to which you want to assign the Station Hunting after Coverage capability.
2. In the **Hunt After Coverage** field, perform one of the following actions:
   - If you want the system to check the station-hunting chain of the last extension in the coverage path, if the system does not find an idle station in the coverage path, type `y`.
   - If you want the system to leave the call at the last available point in the coverage path, type `n`.
3. Select **Enter** to save your changes.

Assigning a hunt-to station to an extension

Procedure

1. Enter `change station n`, where *n* is the number of the extension to which you want to assign a hunt-to station.
2. In the **Hunt-to Station** field, perform one of the following actions:
   - Type the extension that you want the system to check for an idle status, if the extension is busy.
   - If you do not want the system to check further for an idle extension, if the extension that you specified in Step 1 is busy, leave the field blank.
3. Select **Enter** to save your changes.

Administering Station Hunting before Coverage

Procedure

1. Enter `change system-parameters coverage-forwarding`.
2. In the **Station Hunt Before Coverage** field, perform one of the following actions:
   - To enable the Station Hunting Before Coverage capability for your system, type `y`.
   - To disable the Station Hunting Before Coverage capability for your system, type `n`.
3. Select **Enter** to save your changes.

Reports for Station Hunting

The following reports provide information about the Station Hunting feature:

- The List Usage report shows all the extensions that use an extension as the hunt-to-station.

For detailed information on these reports and the associated commands, see *Avaya Aura® Communication Manager Reports*.

Interactions for Station Hunting

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

Remember that the system checks the station-hunting chain only for idle and available extensions.

Adjunct Switch Applications Interface (ASAI)

The system checks the station-hunting chain when ASAI routes a call to an extension with a hunt-to station.

Automatic Call Distribution (ACD)

An agent extension can be part of a station-hunting chain. The system checks the station-hunting chain of the agent only when the caller places the call directly to the agent extension. The system does not check a station-hunting chain for calls that the system routes through hunt groups to an ACD agent.

The system does not check a station-hunting chain for calls that are made to an extension for a logical agent.

Automatic Callback

The system does not check the station-hunting chain of the called extension when the call is a callback-return call.

Bridged Appearance

The system checks the station-hunting chain of an extension if the principal station does not have a call appearance at which the call can terminate. The system checks the chain, even though the extension has available bridged appearances on other stations.

Busy Verification

The system does not check a station-hunting chain for busy-verify calls.

Call Coverage

Call Coverage has precedence over Station Hunting.

The system uses Station Hunting for the last coverage point of the last station in the station-hunting chain under the following conditions:

- The **Hunt After Coverage** field, on the Call Coverage screen is set to y.
- The last coverage point is unavailable because the coverage point is busy, or no one answers the call.
- The last coverage point is a station that has an assigned hunt-to station.
- No one in the coverage path answers the call.

  Coverage Don't Answer covers the call after the system checks the station-hunting chain, if the call can terminate at the coverage point, but no one answers the call.

  If Station Hunting before Coverage is enabled on your system, the system checks the station-hunting chain of the called extension, before the system routes the call to the coverage path of the called extension.

  The system routes the call to the coverage path of the called extension unless the called extension is associated with an XDID telephone. If the called extension is associated with an XDID telephone, the system routes the call to the coverage path of the non-XDID extension in the hunt-to field of the XDID station.

Call Detail Recording (CDR)

CDR records the called extension, and not the extension of the user who answers the call.

Call Forwarding

Call Forwarding has precedence over Station Hunting.

If an idle station has Call Forwarding active, the system forwards the call. If a busy station has Call Forwarding active, the system forwards the call. If the forwarded-to station is busy, the call follows the station-hunting chain of the forwarded-to extension.

Call Park

The system does not check a station-hunting chain for callpark-return calls.

Call Pickup

Station Hunting does not change the operation or the characteristics of Call Pickup.

Call Vectoring

You cannot type a vector directory number (VDN) as a hunt-to station.

If the system encounters with cov y in a **route-to** command, the system routes a call to a busy station to the station-hunting chain of the station. The system does not route the call to the

coverage path of the station. For more information, see the *Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*.

Call Waiting and Attendant Call Waiting

Station Hunting has precedence over Call Waiting.

If a called extension has Call Waiting active, and the extension is already busy on a call, the system checks the station-hunting chain. If the system cannot terminate the call to a station in the station-hunting chain, the call waits at the called extension.

Class of Restriction (COR)

The system checks the COR of the called extension. The system does not check the COR of the stations in a station-hunting chain.

Distributed Communications System (DCS)

Station Hunting is not a DCS feature. All stations in a station-hunting chain must be on the same server that runs Communication Manager.

Do Not Disturb

If Do Not Disturb is active at a station, the system does not check a station-hunting chain for a call to the station.

Extension Number Portability (ENP)

You cannot assign a remote ENP extension as a hunt-to station.

Hunting and Hunting Group

You cannot assign a direct departmental calling (DDC) or uniform call distribution (UCD) extension as a hunt-to station.

Intercom Call

The system denies Station Hunting for intercom calls to a busy extension.

Leave Word Calling (LWC)

If a caller starts LWC, the LWC message is left at the called extension even if the system uses Station Hunting in an attempt to complete the call.

Multimedia

Calls to multimedia endpoints must convert to voice before the system checks a station-hunting chain for the call.

Night Service

The system denies Station Hunting when a night service call is made to a busy night-console extension.

Outgoing Trunk Queueing (OTQ)

The system does not attempt Station Hunting for an OTQ callback-return call.

Personal Central Office Line (PCOL)

The system does not attempt Station Hunting for a PCOL call.

Personal Station Access (PSA)

The system considers a station with PSA dissociated as busy and bypasses the station in the station-hunting chain.

Priority Call

The system denies Station Hunting for priority calls.

Restriction

The system applies proper intercept treatment to a restricted, called extension. Note that the system does not check restrictions on hunt-to stations.

Send All Calls

Send All Calls coverage takes precedence over Station Hunting.

The system applies normal tenant restrictions to a call to the called extension. Note, however, that the system does not check tenant restrictions on hunt-to stations.

Tenant Partitioning

Terminal Translation Initialization (TTI)

The system considers a station with TTI separation as busy and bypasses the station in the station-hunting chain.

Terminating Extension Group (TEG)

You cannot assign a TEG as a hunt-to station.

Uniform Dial Plan (UDP)

You cannot assign a remote UDP extension as a hunt-to station.

X-ported extension

You can assign a hunt-to station to a station that is administered with x in the **Port** field of the Station screen. The system bypasses a hunt-to station that is administered with an x in the **Port** field of the Station screen.

Chapter 172: Station Lock

Use the Station Lock feature to lock a telephone to prevent others from placing outgoing calls from the telephone.

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.

Station Lock by time of day

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

Table continues…

Screen name	Purpose	Fields
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**

End-user procedures for Station Lock

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Activating or deactivating Station Lock from a remote telephone

Procedure

1. Dial a valid barrier code.

   The system generates a dial tone.
2. Dial the Feature Access Code (FAC) for Station Lock.
3. Dial the extension number.
4. Dial the Station Security Code (SSC).

Interactions for Station Lock

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

Attendant Console

You cannot lock an attendant console, but you can lock a digital station that has console permissions.

You can dial the Feature Access Code (FAC) for Station Lock from the attendant console to remotely activate or deactivate Station Lock for another telephone.

Personal Station Access (PSA)

You can use Station Lock to lock a PSA telephone, if the telephone has an extension. When a telephone is dissociated, you cannot activate Station Lock from the telephone.

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.

Station Lock Enhancements

Communication Manager Release 5.2 or later makes more restrictions available on the Station Lock feature. When the Hot Desking Enhancement feature is activated, the following are restricted:

- Access to telephone capabilities (applies to 96xx and 96x1 H.323 IP telephones with firmware changes)
- Call log
- Avaya menu
- Contact list
- USB access
- Redial button
- Bridging on Extension to Cellular calls
- Access to bridged appearances

Additionally, enabling the HDE feature by using the **Hot Desking Enhancement Station Lock** field in the Feature-Related System Parameters screen locks further capabilities. The capabilities are distributed among the telephone and Communication Manager.

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 173: Station Security Code

Use the Station Security Code (SSC) to deny other users access to the functions that are associated with the station. Each station user can change their own SSC if they know the station's current settings.

Detailed description of Station Security Code

Use the Station Security Code (SSC) to deny other users access to the functions that are associated with the station. Each station user can change their own SSC if they know the station's current settings.

SCC enhances system security. To use SCC, you must provide each user with an individual SSC. You can also create a system-wide Feature Access Code (FAC) that users can use to change the individual SSC. A user cannot change a blank SSC.

Station Security Code administration

The following task is part of the administration process for the Station Security Code feature:

- Creating a Station Security Code

Related links

Creating a Station Security Code on page 1291

Screens for administering Station Security Code

Screen name	Purpose	Fields
Feature Access Code (FAC)	Set the access code for the feature.	Station Security Code Change Access Code
Security-Related System Parameters	Set the minimum length of the code.	Minimum Station Security Code Length
Station	Set the code for the station extension.	Security Code

Creating a Station Security Code

Procedure

1. Enter `change feature-access-codes`.
2. Type `#5` in the **Station Security Code Change Access Code** field.

   This action sets the access code for this feature.
3. Save the changes.
4. Enter `change system-parameters security`.
5. In the **Minimum Station Security Code Length** field, type `7`.

   This action determines the minimum required length of the station security codes that you enter on the Station screen. Longer codes are more secure. If you use station security codes for external access to telecommuting features, Avaya recommends that you use a minimum length of 7 digits.
6. Select **Enter** to save your changes.
7. Type `change station n`, where *n* is the extension that you configured for a feature. For the complete list of features for which you can create SSCs, see *Interactions for Station Security Code*.
8. Type a number in the **Security Code** field that is equal in length to the number of digits that you entered in the Security-Related System Parameters screen in Step 5.
9. Save the changes.

Interactions for Station Security Code

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

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

- Call Forwarding
- Demand Printing
- Extended User Administration of Redirected Calls
- Extension to Cellular
- Leave Word Calling (LWC)
- Personal Station Access (PSA)
- Posted Messages
- Registering H.323 phones

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

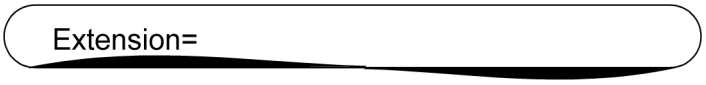
End-user procedures for Station Security Code

You can change the Security Code after the system administrator enables the feature on the Feature Access Code (FAC) screen.

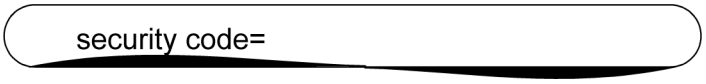
Changing the Station Security Code

Procedure

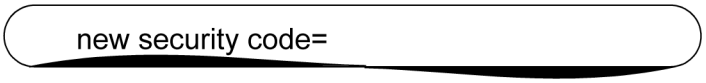
1. After dialing the Feature Access Code (FAC), you can hear a dial tone, and the system displays the following text:

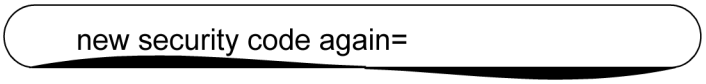
   The system displays this text together with the dialed digits until the number is complete.
2. After this, you receive no dial tone but the display prompts:

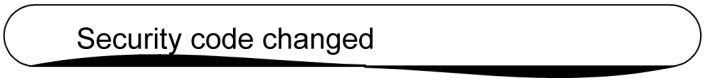
   The system displays the typed-in security code as asterisks (*).
3. Then you receive dial tone and the display prompts:

   The system displays the typed-in security code as asterisks (*).
4. Then you receive dial tone and the display prompts:

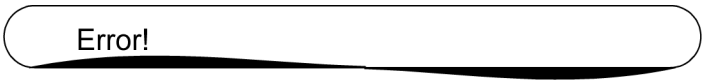
   The system displays the typed-in security code as asterisks (*).
5. You receive acknowledgement from the confirmation tone (3-beep) and additionally the system displays the text as follows:

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

Exception Handling

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



Error!

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

Chapter 174: Suite Check-in

With Suite Check-in, Communication Manager automatically checks in more than one telephone with one check-in command (whether from your PMS or from Communication Manager).

When a room telephone is checked in, Communication Manager looks for a hunt-to extension associated with that station. If it finds one, Communication Manager also checks in the station found in the hunt-to field. Communication Manager also:

- removes controlled outward restriction
- adds the guest's name to the station record for that extension
- stores the call coverage path
- removes any Leave Word Calling (LWC) messages
- marks the room as occupied

If the hunt-to (second or subsequent) station has an extension in its hunt-to field, that station also is checked in. Communication Manager continues checking in stations until it meets a station in the chain with a blank hunt-to field.

Interactions for Suite Check-in

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

Automatic Selection of DID Numbers for Guest Rooms

If Automatic Selection of DID numbers is active, then a DID number is assigned only to the initial extension (the one that appears in the check-in message), not to all of the hunt-to extensions.

Dial By Name

Since the secondary telephones that are checked-in insert a "*" before the name, the system does not display the name when Dial By Name is used. However, the system displays the name (with the "*" in front of it) when the telephone dials the attendant or another display set.

Do Not Disturb

When Do Not Disturb is activated for a telephone, it is active for just that telephone and not other telephones in the hunt-to chain.

Housekeeping Status Change

When a room status feature access code is dialed, the room status is updated only for the extension from which the code was dialed (not the hunt-to telephones as well). Housekeeping should be instructed to dial the room status changes from the primary telephone.

Chapter 175: Supporting TTY Callers

Use the Supporting TTY Callers feature to enable callers to use a teletypewriter device (TTY) to listen to announcements that play TTY recordings. You can also use this feature to set up hunt groups for TTY callers, and to create vectors that process both TTY callers and voice callers.

TTY is also known as TDD (Telecommunications Device for the Deaf).

Detailed description of Supporting TTY Callers

Reliable transmission of TTY information complies with the requirements and guidelines that are outlined in United States accessibility-related laws. Those laws include:

- Titles II, III, and IV of the Americans with Disabilities Act (ADA) of 1990.
- Sections 251 and 255 of the Telecommunications Act of 1996.
- Section 508 of the Workforce Investment Act of 1998.

Communication Manager TTY support is currently restricted to TTY devices that use either the:

- US English standard TTY protocol, specified by ANSI/TIA/EIA 825 as: “A 45.45 Baud FSK modem.”
- UK English standard TTY protocol, Baudot 50.

Important characteristics of the standards are:

- TTYs are silent when not transmitting. Unlike fax machines and computer modems, TTYs have no “handshake” procedure at the start of a call, nor do they have a carrier tone during the call. This approach has the advantage of permitting TTY tones, DTMF, and voice to be intermixed on the same call.
- The ability to intermix voice and typed TTY data on the same call. The most common usage is by people who are hard of hearing, but who can speak clearly. These people often prefer to receive text on a TTY device, and then speak in response. This process is referred to as Voice Carry Over (VCO).
- Operation is “half duplex.” TTY users must take turns transmitting and typically cannot interrupt each other. If two people try to type at the same time, two TTY devices might show no text at all or show text that is unrecognizable. Also, no automatic mechanism exists to let TTY users know when a character that the user correctly typed was received incorrectly.

- Each TTY character consists of a sequence of seven individual tones. The first tone is always a “start tone” at 1800 Hz. This tone is followed by a series of five tones, at either 1400 or 1800 Hz, which specify the character. The final tone in the sequence is always a “stop tone” at 1400 Hz. The stop tone is a border that separates this character from the next.

The following types of systems support TTY communication:

- Analog telephones and trunks
- Digital telephones and trunks
- VoIP gateways
- Messaging systems
- Automated attendant systems
- Interactive Voice Response (IVR) systems
- Wireless systems in which a TTY-compatible coder is used

Announcement set up for TTY callers

TTY devices typically resemble a laptop computer. TTY devices have a one line-or a two-line alphanumeric display, instead of the computer screen.

You record announcements for TTY callers in the same way as you record voice announcements. However, instead of recording from the handset of your telephone, you record from a TTY device. The device is attached to your telephone. You use an n acoustic coupler into which you place the telephone handset or by plugging the TTY device directly into the back, if it is a digital telephone. After calling the announcement extension, and pressing 1 to record. To use the device, you type the announcement using the TTY device.

If you use an acoustic coupler to connect your telephone for recording, you can record TTY and voice into a single announcement. In this case, when you press `1` to record, you can type the TTY message, then immediately pick up the handset to record the voice message. For this type of recording, digital telephones also offer the option to press `#` to complete the recording, which eliminates any extraneous noise at the end of the recording. Unfortunately, using this method for combined TTY and voice recordings is likely to create extraneous noise in the middle of your announcements.

As a alternative to recording with your telephone, you can create `.WAV` files on other recording applications and you can then copy and save the `.WAV` files to your announcement board.

Hunt group set up for TTY callers

In a call center, TTY callers can be accommodated by a hunt group that includes TTY-equipped agents. Although many TTYs can connect directly with the telephone network by way of 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 can speak clearly. These individuals often prefer to receive calls on a TTY and then speak in response. This

requires the call center agent to alternate between listening on the telephone and then typing on the TTY. An acoustically coupled configuration makes this process considerably easier.

Although TTY-emulation software packages are available for personal computers, most of these packages 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, follow the same steps as with voice recordings from your telephone. However, instead of speaking into your telephone to record, you type the announcement with the TTY device.

For an alternative to creating a TTY hunt group, you can use vectors to process TTY calls. With vectors, TTY callers and voice callers can use the same telephone number. In this case, you can also record a single announcement that contains both TTY signaling and a voice recording.

Vectors for TTY calls

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 prerecorded announcements. The ability to provide a hybrid voice-and-TTY announcement, when combined with the automated attendant vectoring capability, can permit a single telephone number to accommodate both voice and TTY callers.

Example of handling TTY calls with vectors

This example shows a vector with which 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 dial 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).

In this 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 actions occur:

1. After a short burst of ringing, a quick burst of TTY tones is sent to the caller to tell the caller to hold, HD. Then a voice announcement is played 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 does not hear the voice announcement, but because the step collects digits, the caller can dial 1 from a 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 this 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, the caller hears silence from vector step 9, and then the announcement in vector step 10, and is then looped back to wait with silence by vector step 11.

Chapter 176: Team Button

Use the Team Button feature to monitor members of a team of stations. The Team Button feature is a standard feature starting with Communication Manager Release 4.0.

Detailed description of Team Button

The Team Button feature is used to monitor the members of a team of stations.

Team Button has two functions:

- Display function

  The monitoring station can observe the state of the monitored station. The indicators depend on the station type and can be a green and red button LED or an icon on the display. For SIP endpoints, the indicators can be both LED and an icon on the display. The ringing of a call on a monitored station might be indicated with audible ringing.

  The monitoring station does not display calls from the monitoring station to the monitored station, regardless of whether the calls are established by pressing the **team** button or by dialing.

  In Communication Manager 6.2, if the monitored station activates redirection, the monitoring station is notified about the redirection only if the monitoring station is the first redirection point. The other monitoring stations are not informed about the redirection state of the monitored station. With Communication Manager 6.3 or later, if the monitored station activates redirection, the monitoring station that is not the reroute destination point, but has the **TEAM_BUTTON_REDIRECT_INDICATION** flag set to `1` in the `46xx_setting` file, gets the redirection notification on the station. The `46xx_setting` file is applicable only to the SIP phones.

- Execution function

  The **team** button can be used as a Speed Dial button or Call Pick-Up button. Depending on the state of the monitored station, when the **team** button on the monitoring station is pushed, a call to the monitored station is established directly or a ringing call is picked from the monitored station.

Speed dialing

- When the monitored station is accessed from the monitoring station through speed dialing, the type of ringing on the monitored station can be configured as priority ringing or intercom ringing. For more information, see *Administering Priority Ring for Speed dialing*.
- Speed dialing is treated as enbloc dialing to avoid time-outs in case of multilocation and mixed-length dial plans.
- When the monitoring station is active on a call, pressing the **team** button puts the active call on hold and a call is established with the monitored station. The call can be transferred by pressing the transfer button. On call transfers, any active Send All Calls (SAC), Call Forwarding (CFWD), and Enhanced Call Forwarding (ECF) settings on the monitored station are overridden. However, coverage criteria are not overridden.

Call Pickup

- If the overall call state of the monitoring station is idle, call pickup can be handled by pressing the **team** button on the monitoring station one time and then going off-hook.

  The first press of the **team** button displays details of the call on the monitored station. If more than one call is ringing on the H.323 monitored station, details of other calls can be viewed by clicking **Next**. When two monitoring stations press the **team** button of the same monitored station, call details are displayed on both the monitoring stations, but the station that first goes off hook or presses the SPEAKER button answers the call.

You can administer H.323 and SIP stations as monitoring and monitored stations.

The following station types are allowed as valid monitored stations, but not as monitoring stations:

- Analog stations
- BRI-stations
- X-ports
- X-mobiles

The number of **team** buttons for each station is 31. However, the number of stations that other stations can monitor is limited to a maximum of 15. In effect, the maximum number of **team** buttons in a system is 15, that is, each station can supervise and work on a maximum of 15 stations.

Team Button is a station oriented feature, not a call appearance oriented feature. You must consider all call appearances on a station as one call appearance of that station. The option to use the name of the monitored station name instead of the extension is available.

Audible Ringing and Call States for Team Button

A monitored station can have two call states and two ringing states. The call states and ringing states are displayed separately on the monitoring station:

The call states are:

- IDLE – All primary call appearances are in an idle state.

- BUSY – One or more call appearance have a state which is different to idle.

Note:

A ringing station is considered as a station with the idle overall call state.

The busy states are as follows:

- Off-hook
- Dialing
- Calling
- Active
- Hold
- Soft hold (used for conference and transfer steps)

The overall ringing states are as follows:

- IDLE – No incoming call appearance is ringing
- RINGING – One incoming call appearance is ringing, silent ringing or audible ringing
- DOUBLE RINGING – More than one incoming call appearance is ringing, silent ringing or audible ringing.

Direct transfer

Direct transfer is a single-click operation to complete the transfer operation when the second call is initiated using the **team** button. If the user of a monitoring station is active on a call and makes another call by using the **team** button, Communication Manager treats the **team** button as an implicit transfer initiate request. On pressing the **Transfer complete** softkey on the monitoring station, the call gets transferred to the monitored station.

Note:

Only one-X SIP stations support Direct transfer. 96xx and 96x1 H.323 stations do not support this feature. SIP stations do not support the following transfer features:

- Abort transfer
- Pull transfer
- Pickup on transfer

Team Button administration

The following tasks are part of the administration process for the Team Button feature:

- Configuring the Team Button
- Viewing the status of Team Button usage
- Viewing system capacity for Team Button

Configuring the team button for H.323 and DCP stations

Procedure

1. Enter `change station xxxx`, where *xxxx* is the extension of the station that you want to administer.
2. In the **Button Assignments** section, in a blank field, type `team`.
3. In the **Ext** field, type the extension of the monitored station.
4. In the **Rg** field, type one of the following values:
   - `a`: abbreviated-ring
   - `d`: delayed-ring
   - `n`: no-ring
   - `r`: ring
   - `i`: intercom

Configuring the team button for SIP stations

Procedure

1. Log on to the System Manager web console.
2. Click **Elements** > **Communication Manager**.
3. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
4. Select the Communication Manager instance.
5. Click **Show List**.
6. In the **Endpoint List** section, select the endpoint that you want to edit.
7. Click **Edit**.
8. Click the **Button Assignments** tab.
9. Select **team**.
10. In the **Ext** field, type the extension of the monitored station.

11. In the **Ring** field, type one of the following values:
    - `a` or `abbreviated-ring`
    - `d` or `delayed-ring`
    - `n` or `no-ring`
    - `r` or `ring`
    - `i` or `icom`

Viewing the status of Team Button usage

Procedure

1. Enter `list usage extension` *xxxx*, where *xxxx* is the extension.
2. Page down till you see the fields for Team Button Assigned in Station.

   You can view the extension numbers and button assignments for each extension on this page.

Viewing system capacity for Team Button

Procedure

1. Enter `display capacity`.
2. Page down till you see the **Team button/Monitored Stations** field.

   You can view the used, available and system limit for Team Buttons for your system.

Administering Team Button audible ringing

Procedure

1. Enter `change cor`.
2. Click **Next** till you see the **Team Btn** fields.
3. To disable audible ringing on the monitoring station, set **Team Btn Silent if Active** field to `y`.
4. Select **Enter** to save your changes.

Administering Team Button Priority Ring for speed dialing

Procedure

1. Enter `change cor`.
2. Click **Next** till you see the **Team Btn** fields.
3. To enable priority ringing, set **Priority Ring** field to `y`.
4. Select **Enter** to save your changes.

Administering Team Button display of station name

Procedure

1. Enter `change cor`.
2. Click **Next** till you see the **Team Btn** fields.
3. To enable display of monitored station name instead of the number, set **Team Btn Display Name** field to `y`.
4. Select **Enter** to save your changes.

Administering Team Button Call Pickup by going off hook

Procedure

1. Enter `change cor`.
2. Click **Next** till you see the **Team Btn** fields.
3. To enable pick up of a call by going off-hook, set the **Pick Up by Going Off Hook** field to `y`.
4. Select **Enter** to save your changes.

Team Button Override Send All Calls/Call Forward

From Communication Manager Release 5.1 onwards, you can activate the Team Button feature to use its speed dial function and to override a rerouting caused by active Send All Calls (SAC), Call Forwarding (CFWD) all, or Enhanced Call Forward (ECF) unconditional.

When the team button is pressed on the monitoring station and the monitored station has a direct rerouting active (SAC, CFWD all, ECF unconditional), the call may do any of the following, depending upon administration:

- Be rerouted
- Ring the monitored station
- Display a message asking the caller which of (1) or (2) to do

Dialing the number of the team member is handled by pressing a team button.

The monitored station with active rerouting is able to disallow overriding in general.

The monitoring station must be a member in a class in which overriding of SAC/CFWD is allowed.

The functionality is controlled by:

- COR settings
  - monitoring station: SAC/CR Override by Team Btn
  - monitored station: SAC/CF Override Protection for Team Btn

- Setting on monitoring station form
  - SAC/CF override [a(sk), n(o), y(es)]

The settings on the station form of the monitoring station are:

- n(o) – cannot override rerouting. The station cannot override rerouting.
- y(es) – can override rerouting. The station has the ability to override the rerouting the monitored station has set, as long as one incoming call appearance is free. If no free call appearance is available, the call fails and the user of the monitoring station hears busy tone.
- a(sk) – ask whether the user wants to follow the rerouting or override it. When the user of the station can decide whether rerouting should take place or not, a message is sent to the station which displays the active rerouting and the number of the forwarded station. The user of the monitoring station can now follow the rerouting by dialing “1” or “#”, or by letting the timer which supervises the team button pushes expire, or overriding the active rerouting by dialing “0” or “*”.

No Team Button Override of SAC/CFWD

COR of monitoring station: SAC/CF Override by Team Btn	COR of monitored station: SAC/CF Override Protection for Team Btn	Monitoring station form: SAC/CF override
no	no/yes	ask/no/yes
yes	yes	ask/no/yes
yes	no	no

Using speed dialing by pressing the team button on the monitoring station doesn’t establish a call to the monitored station (with active SAV, CFWD all, or ECF unconditional), but follows the assigned active rerouting.

Unconditional Team Button Override of SAC/CFWD

COR of monitoring station: SAC/CF Override by Team Btn	COR of monitored station: SAC/CF Override Protection for Team Btn	Monitoring station form: SAC/CF Override
yes	no	yes

Using speed dialing by pressing the team button on the monitoring station establishes a call to the monitored station (with active SAC, CFWD all, or ECF unconditional) instead of following the active rerouting.

If the monitored station does not answer the call within 30 seconds, the call is rerouted to the assigned rerouting destination.

Team Button override of SAC/CFWD by Asking

COR of monitoring station: SAC/CF Override by Team Btn	COR of monitored station: SAC/CF Override Protection for Team Btn	Monitoring station form: SAC/CF Override
yes	no	ask

Using speed dialing by pressing the team button on the monitoring station neither establishes a call to the monitored station (with active SAC, CFWD all, or ECF unconditional) nor reroutes the call to the assigned rerouting destination.

Instead, a message is displayed on the station which shows the rerouting destination and asks the user of the station if the user wants to follow the rerouting or override it.

Dialing digits or pressing any other button by the user of the station leads to a result as follows:

- Dialing 1 or #: rerouting
- Dialing 0 or *: overriding of rerouting
- No action within 9 seconds: rerouting
- Exit button: rerouting
- Drop button: end of call establishment
- Almost any other digit or button press: no reaction and timer (9 seconds) is restarted

If rerouting is overridden and the monitored station does not answer the call within 30 seconds, the call is rerouted to the assigned rerouting destination.

Interactions for Team Button

Limit Number of Concurrent Calls

If the user of a monitoring station presses the **team** button and the monitored station that has Limit Number of Concurrent Calls enabled is busy on a call, the monitoring station receives a busy tone.

Coverage path

If the user of a monitoring station presses the **team** button and the monitored station has coverage path enabled with the monitoring station as the first destination in the coverage path, the forwarding is ignored and the call is made to the monitored station.

Personal Station Access

If the user of an H.323 or DCP monitoring station presses the **team** button and the monitored extension does not have an associated phone, the call is rejected.

Group

The monitored station can be a member of a hunt group, a terminating extension group, or a personal-CO-line group. If the user of a monitoring station presses the **team** button administered with the group extension number of the monitored station, the call is established only if the monitored station has an idle call appearance.

OPTIM

If the user of a monitoring station presses the **team** button and the monitored station has an Off-PBX Telephone Integration and Mobility (OPTIM) user, the call rings at the monitored station and the OPTIM station.

Bridged Call Appearance

If the user of a monitoring station presses the **team** button and the monitored station has bridged call appearance on another station, the call rings at the monitored station and the station with the bridged appearance.

Dual Registration

Dual registration is not supported with Team Button.

Multi-Device Access

In Communication Manager 6.3 or later, Team Button is supported on the SIP endpoints registered with the same extension.

1xC SIP in shared control mode

In Communication Manager 6.3 or later, Team Button is supported on Avaya one-X® Communicator for Windows SIP endpoints in the shared control mode and the deskphone mode.

Chapter 177: Telephone Display

Use the Telephone Display feature to provide users of multiappearance telephone with current call and message information. The system displays the information that depends on the type of display that the user selects with the buttons on the telephone.

Users can use the features of the telephone to retrieve stored information, such as messages and directory information. You can select English, French, Italian, Spanish, user-defined, or Unicode languages to display the messages or the information.

Detailed description of Telephone Display

Users can use the features of the telephone to retrieve stored information, such as messages and directory information. You can select English, French, Italian, Spanish, user-defined, or Unicode languages to display the messages or the information.

With Enhanced telephone display, you can choose the types of characters for the telephone display of the user. You can administer the software to display Roman (European) characters, or Cyrillic (Russian), Katakana (Japanese), or Ukrainian characters. The type of telephones that your company uses determine the character sets that you can display.

Button display modes

You can assign several display modes to telephone buttons. To access these modes, users press the assigned button on the telephone. All the buttons are administrable.

Button mode	Function
Normal	Displays call-related information for the active call appearance. This information includes call appearance, and the name and the number of the calling party or the called party, depending on the type of call. Can also displays elapsed time when the display is in normal mode. The system shows the elapsed time in hours, minutes, and seconds. Timing starts and stops when the button is pressed.
Inspect	Displays call-related information for an incoming call when the user is active on a different call appearance. Users must reset the mode manually for each call.

Table continues…

Button mode	Function
Stored Number	Displays one of the following numbers: • The last number that the user dialed (Last Number Dialed) • The number that is stored in an Abbreviated Dialing button that is administered to the telephone • A number that is stored in an Abbreviated Dialing list • A number that is assigned to a button that is administered by Facility Busy Indication
Date and Time	The current date and time of day.
Integrated Directory	Turns off the touchtone signals so that the user can use the touchtone buttons to enter the name of a system user. After the user enters a name, the display shows the name and the extension. Integrated Directory can use one additional related button: • Call-Disp automatically returns the call that is requested by the currently displayed message or the currently displayed name and extension. Note, if the name was entered with tildes as the first two characters the name will be hidden (when Display Character Set = roman) and is not sent to a telephone with any integrated directory search.
Message Retrieval	Retrieves messages for telephone users. If no messages are stored, the display shows `NO MESSAGES`. Users can retrieve messages even if the retriever is active on a call. Message Retrieval can use 3 additional related buttons: • Next Message retrieves the next message, or displays End of File, Push Next To Repeat when in Retrieval mode. • Call-Disp automatically returns the call that is requested by the currently displayed message or the currently displayed name and extension. • Delete deletes the currently displayed message.
Coverage Message Retrieval Mode	Retrieves messages for users of the telephone users who do not have a display module. You must administer retrieval permission for a user to retrieve messages of other users. The user does not need to lift the handset to retrieve messages. The user can retrieve messages even if the retriever is active on a call. Coverage Message Retrieval can use three additional related buttons: • Next Message retrieves the next message, or displays End of File, Push Next To Repeat when in Retrieval mode. • Call-Disp automatically returns the call that is requested by the currently displayed message or the currently displayed name and extension. • Delete deletes the currently displayed message.

Integrated Directory

With the Integrated Directory feature, users can retrieve a party's extension number by keying in the name of the required party on the touch-tone pad. Once the required party is found, a

call can be placed to that party by simply pressing the CALL button. The Integrated Directory is a Personal-Service Display Mode, adding to the list of Message-Retrieval, Coverage-Message-Retrieval, Stored-Number, and Date/Time modes. This Integrated Directory feature now provides the ability to look up names with international characters (Latin letter with a diacritic) when Display Character Set = Roman.

When you set the **Display Character Set** field on the System-Parameters Country-Options screen to Katakana, the following is valid:

- Names with Roman and Katakana characters are stored in the integrated directory.
- The integrated directory does not support a search using Katakana characters. If you want to view names with Katakana characters, enter the wildcard "*" and then use the **next** key.
- In the integrated directory, names that begin with Roman characters followed by Katakana characters (for example, Hirohito ヒロヒト) can be searched using the Roman characters in the name.

Integrated Directory Data Base

Station users' names are entered from the System Administration Terminal. If you want the station user name to be hidden from the Integrated Directory feature, the name should be entered with '~~' as the first two characters of the name. Names entered in this way are not added to the Integrated Directory Database. The Integrated Directory feature only retrieves names that are in the Integrated Directory Database.

INTEGRATED DIRECTORY Mode Button

An INTEGRATED DIRECTORY mode button is provided to activate the Integrated Directory service.

With the Integrated Directory feature, you can do the following changes:

- The ability to hide names (Display Character Set = Roman) can only be accomplished if the name begins with two tildes. Before Communication Manager 4.0, other symbols might have been used to hide names. This is no longer supported. If your site was using a symbol other then the tilde to hide names, the recommended upgrade procedure is to export such names to a `.csv` file. You must do a global change on the symbol you used replacing such symbol with two tildes. After making the change, import the data back to your Communication Manager server.
- Before Communication Manager 4.0, the asterisk was used as a wild card to skip the comma in Integrated Directory names such as "Doe, John." The comma is now supported on button 1 and so the one key should be pressed rather then the asterisk key when you want to move past the comma in any Integrated Directory name.

When the **Display Character Set** field on the System-Parameters Country-Options screen is set to Cyrillic or Ukrainian:

- Names are stored in a Roman or a Cyrillic integrated directory. If a name includes a tilde (~) the name is stored only in the Cyrillic integrated directory. If not, the name is stored in the Roman integrated directory.

- The integrated directory searched is determined by the value (Roman or Cyrillic) in the Directory Search Sort Order of the System-Parameters Country-Options screen.
- While in the integrated directory feature, Communication Manager interprets **#** key as an instruction to switch the Directory Search Sort Order to the non-administered value when the **#** key is pressed before any other dialpad keys: 1,2,3,4,5,6,7,8,9,*,0. The **#** key is ignored if it is not the first dialpad key pressed. This switch to the non-administered value only stays in effect during the current integrated directory feature session. So the next invocation of the integrated directory feature uses the administered value.

The table on page 1312 shows the characters assigned to Dial Pad Keys when Display Character Set = Roman.

Table 89: Dial Pad International Character Assignment

Key	Characters Assigned
0	0 space
1	, . @ 1
2	a A á Á à À ă Ă â Â å Å ä Ä ã Ã ą Ą æ Æ b B c C ć Ć č Č ç Ç 2
3	d D Ď ð Đ e E é É è È ě Ě ê Ê ë Ë ė Ė ę Ę f F 3
4	g G ğ Ğ h H i I í Í ì Ì î Î ï Ï 4
5	j J k K l L ĺ Ľ 5
6	m M n N ń Ń ň Ň ñ Ñ o O ó Ó ò Ò ô Ô ö Ö ő Ő õ Õ ø Ø 6
7	p P q Q r R ř Ř s S ś Ś š Š ş Ş ß 7
8	t T ť Ţ u U ú Ú ù Ù û Û ù Ù ü Ü ű Ű v V 8
9	w W x X y Y ý Ý ÿ Ÿ z Z ź Ź ž Ž ż Ż Þ þ 9
*	´ ‘ - ! " # $ % & ( ) * + / : ; < = > ? [\ ] ^ _ ` { | }

The table on page 1312 shows the Dial Pad keys when Display Character Set = Cyrillic or Ukrainian.

Table 90: Dial Pad Cyrillic Character Assignment

Key	Character
0	0 *space*
1	, . @ 1
2	a A Á b B Ã 2
3	Ä e E ¨ Æ Ç 3
4	È i I ¯ É k K Ë 4
5	m M h H o O Ï 5
6	p P c C t T y Y 6
7	Ô x X Ö × 7

Table continues…

Key	Character
8	Ø Ù Ú Û 8
9	Ü Ý Þ ß 9
*	‘ - ! " # $ % & ( ) * + / : ; < = > ? [\ ] ^ _ ` { | }

For more information on character mapping for the 9600 IP telephones, see Character Mapping and Text Entry on 9600 IP Telephones, Issue 1, 16-601991.

Call-related information telephone display

The software provides the following call-related information:

Call appearance identification

A lowercase letter is used to designate call appearance buttons on the display. The display shows `a=` for an incoming call on the first button, `b=` for an incoming call on the second button, and so on.

The system might omit the call-appearance information so that the Call Log find capability in the PC/PBX Connection software works properly.

Note:

The displays of IP phones and call logs show whether calls were answered through call pickup from another station, and if the Temporary Bridged Appearance feature is in use. This does not apply to pickup through the **Team** button.

Calling party identification

When a call is from inside the system, the display shows the name of the caller or a unique identification that is administered for the telephone being used, and the extension of the calling party. When the call is from outside the system, the display shows the trunk group name (such as CHICAGO) and the Trunk Access Code (TAC) that is assigned to the trunk group used for the call. If a user is active on a call and receives another call, the display automatically shows the identification of the second caller for a few seconds. The system then automatically restores the display to show the information that is associated with the active call appearance.

For example:

outgoing trunk call

```
b=87843541
```

8 is the TAC, and 784-3541 is the number that was dialed

then

```
b=OUTSIDE CALL                  8
```

or

```
b=WATS                 101
```

Note:

Because of space limitations, some name displays are shortened to 15 characters. These displays include displays for transferred or covered calls, non-DCS, ISDN-PRI calls, VDN service observing displays, LWC messages, or the queue status of an agent.

Called party identification

On calls to a system user, the system displays the digits as the digits are dialed. After dialing is complete, the system displays the name and the extension of the called party. If no name is accessed, the dialed digits remain on the display.

On outgoing calls, the system displays the digits as the digits are dialed. After dialing is complete, the display shows the name and the TAC that is assigned to the trunk group being called. Optionally on a trunk-group basis, the display can show only the dialed digits, not the trunk group name and the TAC.

For example:

Dialed digits

```
a=3602
```

then:

```
a=TOM BROWN              3062
```

or, if no name is available:

```
a=EXT 3602               3062
```

Call purpose

Call purpose identifies the reason for an incoming call or a redirected call. The system does not identify a call purpose for a normal incoming call. The system sometimes display the following identifiers:

Display	Meaning
b - (Busy)	The called user is active on a call, and has a temporary bridged appearance of the call.
c - (Cover All)	The called user has Cover All assigned.
callback	The call is an Automatic Callback call from the system.
d - (Coverage on Don’t Answer)	The call was redirected because the called telephone unanswered. This message also indicates that the called user has a temporary bridged appearance of the call.
f - (Call Forwarding)	Another user has forwarded calls to this telephone.
h - (Station hunt)	The called user is active on a call, and station hunt was used to route the call.
ICOM	The call is an Intercom call.
p - (Pickup)	The user answered the call of a Call Pickup group member.

Table continues…

Display	Meaning
park	The user parked a call.
priority	The call has priority status.
s - (Send All Calls)	The called user is temporarily sending all calls to coverage and the call was redirected to this telephone.

Message retrieval telephone administration

You can designate certain telephones and attendant groups for system-wide message retrieval. Users of these telephones or consoles can retrieve Leave Word Calling (LWC) and call coverage messages for other telephone users. These other users can include Direct Department Calling (DDC) groups, Uniform Call Distribution (UCD) groups, and Terminating Extension Groups (TEGs). Users of these telephones or consoles can also retrieve external call logs. You can assign system-wide retrieving telephones or consoles. Use the Feature-Related System Parameters screen to make these assignments.

Messages for a telephone user can be retrieved at selected telephones, or any attendant console. However, the retriever must be on the call coverage path of the user, and permission to retrieve messages must be assigned for the telephone of the user.

Feature information telephone displays

Telephone displays provide information about the activity on individual telephones and consoles, including confirmation that a certain feature is being used. You administer the language to use for messages on the Station screen for each telephone.

Note:

As of July 1, 2005, new messages are no longer added to the Language Translations screens, so these screens may not show all available Communication Manager messages. As a preferred method for entering translations for user-defined telephone messages, Avaya recommends using the Avaya Message Editing Tool (AMET). This tool is available for download from http://www.avaya.com. Also, to administer Unicode display languages, see the section Unicode display administration on page 120.

Support for unicode “Native Name”

Communication Manager supports Unicode for the Name associated with Vector Directory Numbers (VDNs), trunk groups, hunt groups, and stations. 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.

Note:

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 in *Administering Avaya Aura® Communication Manager*.

Enhanced telephone display

With enhanced telephone display, you can choose the types of characters your telephone displays. You can choose standard Roman characters, or Cyrillic, Katakana, or Ukrainian characters. Your Avaya representative sets the character type on the System Parameters Country-Options screen. The character set that you can display also depends on the telephones that your company uses.

You can choose one of the following character sets for messages on your display telephones:

- Cyrillic contains the characters that are required to display the Russian language. The system displays all Russian characters in uppercase letters.
- Katakana contains the characters that are required to display the Japanese language, and as some European characters and other symbols. The system displays all Japanese characters in uppercase letters.
- Roman contains two character sets:
  - US English contains the Roman alphabet, and the numerals and the special characters that are standard on the US English keyboard. The system displays US English characters in uppercase and lowercase letters.
  - European contains characters for many European languages. The system displays all European characters in uppercase letters.
- Ukrainian contains the characters that are required to display the Ukrainian language. The system displays all Ukrainian characters in uppercase letters.

The type of telephones that your company uses must support the characters that you want to display. Each character set requires specific firmware in the telephone. Ensure that you use telephones with the same firmware type across your entire system. If you do not use telephones with the same firmware type across your entire system, the displays do not appear as expected. Your Avaya representative can ensure that you have the correct telephone types for the characters that you want to display.

This section shows the English, the French, Italian, and Spanish message for each feature. When time is displayed, the English language uses the abbreviations AM and PM. All other languages use 24-hour time.

Telephone features language displays

Table 91: Telephone features

English	French	Italian	Spanish
AUTO WAKEUP - Ext: xxxxx Time: --:-- xM	REVEIL AUTO. - POSTE: xxxxx HEURE: --:--	SERVIZIO SVEGLIA - Tel: xxxxx Ora: --:--	DESPERT AUTOMA - EXT: xxxxx HORA: --:--
INVALID EXTENSION - TRY AGAIN	NUMERO DE POSTE EST ERRONE - REESSAYER	NUMERO ERRATO - RIPETERE	EXTENSION NO VALIDO - INTENTE DE NUEVO
WAKEUP ENTRY DENIED - INTERVAL FULL	DEM. REVEIL REFUSEE - INTERVALLE PLEIN	SVEGLIA NON ATTIVATA - ORARIO OCCUP	ENTRADA DENEGADA - INTERVALO COMPLETO
WAKEUP ENTRY DENIED - NO PERMISSION	DEM. REVEIL REFUSEE - SANS AUTORISATION	SVEGLIA NON ATTIVATA - NON PERMESSO	ENTRADA DENEGADA - SIN PERMISO
WAKEUP ENTRY DENIED - SYSTEM FULL	DEM. REVEIL REFUSEE - ENCOMBREMENT	SVEGLIA NON ATTIVATA - CONGESTIONE	ENTRADA DENEGADA - SISTEMA COMPLETO
WAKEUP ENTRY DENIED - TOO SOON	DEM. REVEIL REFUSEE - TROP TOT	SVEGLIA NON ATTIVATA - TROPPO PRESTO	ENTRADA DENEGADA - MUY PRONTO
WAKEUP REQUEST CANCELED	DEMANDE DE REVEIL EST ANNULEE	RICHIESTA SVEGLIA CANENTRYATA	SOLICITUD DE DESPERTADOR CANCELADA
WAKEUP REQUEST CONFIRMED	DEMANDE DE REVEIL EST CONFIRMEE	RICHIESTA SVEGLIA CONFERMATA	SOLICITUD DE DESPERTADOR CONFIRMADA
WAKEUP CALL	APPEL DE REVEIL	SERV. SVEGLIA	DESPIERTE

ASAI language displays

Table 92: ASAI displays

English	French	Italian	Spanish
YOU HAVE ADJUNCT MESSAGES	MESSAGES SUPPLEMENTAIRES	MESSAGGI AGGIUNTIVI	TIENE MENSAJES ADICIONALES

Busy verification of terminals and trunks language displays

Table 93: Busy verification of terminals and trunks

English	French	Italian	Spanish
ALL MADE BUSY	TOUS OCC.	TUTTI OCCUPATI	TODAS OCUPADAS
BRIDGED	EN DERIVATION	OCCUPATO	PUENTEADA
DENIED	INTERDIT	NON PERMESSO	DENEGADO
INVALID	ERRONE	NON VALIDO	NO VALIDO
NO MEMBER	AUCUN MEMBRE	NESSUN ELEMENTO	NINGUN MIEMBRO
OUT OF SERVICE	HORS SERVICE	FUORI SERVIZIO	FUERA SERVICIO
RESTRICTED	RESTREINT	RISTRETTO	RESTRINGIDO
TERMINATED	TERMINE	TERMINATO	TERMINADO
TRUNK SEIZED	CIRCUIT SAISI	GIUNZIONE IMP.	ENLACE OCUPADO
VERIFIED	VERIFIE	VERIFICATO	VERIFICADO

Call Appearance language displays

For each language, the active call appearance appears as:

“a =” (English)

Call-appearance buttons are shown on the display by a lower-case letter (a through z for the first 26 call appearances), followed by “=.” Lowercase letters A through Z, followed by “=” are used for additional call appearances.

Call Detail Recording language displays

Table 94: Call Detail Recording

English	French	Italian	Spanish
CDR OVERLOAD	SURCHARGE EDA	SVRACCARICO DAC	SOBRECARGA DAT

Call progress feedback language displays

Table 95: Call progress feedback displays

English	French	Italian	Spanish
busy (Extension Busy, Intrusion Not Allowed, Call Waiting Not Allowed)	OCCUPE (Occupe)	occ (Occupato)	OCUPADA (Ocupada)
busy(I) (Extension Busy, Intrusion Allowed, Call Waiting Not Allowed)	OCC.(E) (Entree ligne occupe)	occ(I) (Occupato-Intrusione)	OCUP(I) (Ocupada-intrusion)

Table continues…

English	French	Italian	Spanish
ringing (Extension Ringing)	SONNE (Libre)	libero (Libero)	LIBRE (Libero)
wait (Extension Busy, Intrusion Not Allowed, Call Waiting Allowed)	ATTENTE (Attente)	auat (Autoattesa)	ESPERA (Espera)
(I) wait (Extension Busy, Intrusion Allowed, Call Waiting Allowed)	(E) ATTENTE (Entree ligne attente)	(I) auat (Intrusione-Autoattesa)	(I) ESPERA (Intrusion, en espera)

Class of Restriction (COR) language displays

Table 96: Class of Restriction (COR) displays

Restriction	English	French	Italian	Spanish
Toll	TOLL	INT.	TASS	TARF
Full	FULL	COM.	DISB	LLEN
No Restrictions	NONE	AUC.	ABIL	NING
Origination	ORIG	DEP.	ORIG	ORIG
Outward	OTWD	SOR.	USCN	SALI

Translate time messages

Days of the week format language displays

Table 97: Days of the week format

English	French	Italian	Spanish
SUNDAY	DIMANCHE	DOMENICA	DOMINGO
MONDAY	LUNDI	LUNEDI	LUNES
TUESDAY	MARDI	MARTEDI	MARTES
WEDNESDAY	MERCREDI	MERCOLEDI	MIERCOLES
THURSDAY	JEUDI	GIOVEDI	JUEVES
FRIDAY	VENDREDI	VENERDI	VIERNES
SATURDAY	SAMEDI	SABATO	SABADO

Date and Time mode - time not available language displays

Table 98: Date and Time mode - time not available

English	French	Italian	Spanish
SORRY, TIME UNAVAILABLE NOW	HEURE ET DATE INDISPONIBLES	ORA E DATA TEMPON DISPONIBILI	HORA Y FECHA NO DISPONIBLES AHORA

Months of the year format language displays

Table 99: Months of the year format

English	French	Italian	Spanish
JANUARY	JANVIER	GENNAIO	ENERO
FEBRUARY	FEVRIER	FEBBRAIO	FEBRERO
MARCH	MARS	MARZO	MARZO
APRIL	AVRIL	APRILE	ABRIL
MAY	MAI	MAGGIO	MAYO
JUNE	JUIN	GIUGNO	JUNIO
JULY	JUILLET	LUGLIO	JULIO
AUGUST	AOUT	AGOSTO	AGOSTO
SEPTEMBER	SEPTEMBRE	SETTEMBRE	SEPTIEMBRE
OCTOBER	OCTOBRE	OTTOBRE	OCTUBRE
NOVEMBER	NOVEMBRE	NOVEMBRE	NOVIEMBRE
DECEMBER	DECEMBRE	DICEMBRE	DICIEMBRE

Do Not Disturb (Hotel/Motel feature) language displays

Table 100: Do Not Disturb (Hotel/Motel feature)

English	French	Italian	Spanish
DO NOT DIST - Group: xx Time: --:-- xM	NE PAS DERANGER GROUPE: xx HEURE: --:--	NON DISTURBARE - Grp: xx Ora: --:--	NO MOLESTAR - GRUPO: xx HORA: --:--
DO NOT DIST - Ext: xxxxx Time: --:-- xM	NE PAS DERANGER POSTE:xxxxx HEURE: --:--	NON DISTURBARE - Tel: xxxxx Ora: --:--	NO MOLESTAR - EXT: xxxxx HORA: --:--
DO NOT DIST ENTRY DENIED - INTERVAL FULL	DEMANDE EST REFUSEE - INTERVALLE PLEIN	SERVIZIO NON ATTIVATO - ORARIO OCCUP	ENTRADA DENEGADA - INTERVALO COMPLETO
DO NOT DIST ENTRY DENIED - NO PERMISSION	DEMANDE EST REFUSEE - SANS AUTORISATION	SERVIZIO NON ATTIVATO - NON PERMESSO	ENTRADA DENEGADA - SIN PERMISO
DO NOT DIST ENTRY DENIED - SYSTEM FULL	DEMANDE EST REFUSEE - ENCOMBREMENT	SERVIZIO NON ATTIVATO - CONGESTIONE	ENTRADA DENEGADA - SISTEMA COMPLETO
DO NOT DIST ENTRY DENIED - TOO SOON	DEMANDE EST REFUSEE - TROP TOT	SERVIZIO NON ATTIVATO - TROPPO PRESTO	ENTRADA DENEGADA - MUY PRONTO

Table continues…

English	French	Italian	Spanish
INVALID GROUP - TRY AGAIN	GROUPE ERRONE - REESSAYER	GRUPPO NON VALIDO - RIPETERE	GRUPO NO VALIDO - INTENTE DE NUEVO
THANK YOU - DO NOT DIST ENTRY CONFIRMED	MERCI - DEMANDE EST CONFIRMEE	NON DISTURBARE - RICHIESTA CONFERMATA	NO MOLESTAR - ENTRADA CONFIRMADA
THANK YOU - DO NOT DIST REQUEST CANCELED	MERCI - DEMANDE EST ANNULEE	NON DISTURBARE - RICHIESTA CANENTRYATA	MUCHAS GRACIAS - SOLICITUD CANCELADA

Enhanced Abbreviated Dialing - user defined language translations

Field separator language displays

Table 101: Field separator

English	French	Italian	Spanish
<calling party> “to” <called party>	<calling party> “a” <called party>	<calling party> “a” <called party>	<calling party> “a” <called party>

Directory language displays

English	French	Italian	Spanish
DIRECTORY - PLEASE ENTER NAME	ANNUAIRE - ENTRER LE NOM	ELENCO UTENTI - INTRODURRE NOME	GUIA TELEFONICA - INTRODUZCA NOMBRE
DIRECTORY UNAVAILABLE - TRY LATER	ANNUAIRE INDISPONIBLE - REESSAYER	ELENCO UTENTI TEMP. NON DISPONIBILE	GUIA TEL INDISPONIBLE - INTENTE DESPUES
NO MATCH - TRY AGAIN	INTROUVABLE - REESSAYER	NESSUNA CORRISPONDENZA - RIPETERE	NO CORRESPONDE - INTENTE DE NUEVO

ISDN language displays

Table 102: ISDN

English	French	Italian	Spanish
ANSWERED BY	REPONDU PAR	RISPOSTA DA	RESPONDIDO POR
CALL FROM	APPEL DE	CHIAMATA DA	LLAMADA DE
INTL	INTL	INTL	INTL

Leave Word Calling language displays

Table 103: Leave Word Calling messages

English	French	Italian	Spanish
CANNOT BE DELETED - CALL MESSAGE CENTER	NE PEUT ETRE SUPP./APPELER RECEP. MESS.	NON CANENTRYATO. CHIAMARE CENTRO MESSAGGI	NO ELIMINADO-LLAMA CENTRO DE MENSAJES
DELETED	SUPPRIME	MESSAGGIO CANENTRYATO	ELIMINADO
END OF MESSAGES (NEXT TO REPEAT)	FIN DES MESSAGES (SUIVANT POUR REPETER)	FINE MESSAGGI. <successivo> PER RIPETERE	FIN DE MENSAJES (SIGUIENTE PARA REPITIR)
GET DIAL TONE, PUSH Cover Msg Retrieval	TONALITE D'ENVOI - <LECT. MESS. COUV.>	<rec mess copert> DOPO IL TONO DI CENTR	OBTENGA TONO OPRIMA <RECUP MNSJE COBERT>
IN PROGRESS	EN COURS	ATTENDERE...	EN CURSO
MESSAGE RETRIEVAL DENIED	LECTURE DE MESSAGES INTERDITE	LETTURA MESSAGGIO NON PERMESSA	RECUPERACION DE MENSAJES DENEGADA
MESSAGE RETRIEVAL LOCKED	LECTURE DE MESSAGES BLOQUEE	LETTURA MESSAGGIO BLOCCATA	RECUPERACION DE MENSAJES BLOQUEADA
MESSAGES FOR	MESSAGES POUR	MESSAGGI PER	MENSAJES PARA
MESSAGES UNAVAILABLE - TRY LATER	MESSAGES INDISPONIBLES - REESSAYER	MESSAGGI TEMPORANEAMENTE NON DISPONIBILI	MENSAJES NO DISPONIBLES, INTENTE DESPUES
Message Center (AUDIX) CALL	APPEL DE LA RECEPTION DE MESS. (AUDIX)	Chiamata dal Centro Messaggi (AUDIX)	LLAMADA DEL CENTRO DE MENSAJES (AUDIX)
NO MESSAGES	PAS DE MESSAGES	NESSUN MESSAGGIO	NINGUN MENSAJE
WHOSE MESSAGES? (DIAL EXTENSION NUMBER)	MESSAGES DE QUEL NO.? (ENTRER NO. POSTE)	LETTURA MESSAGGI. INTRODURRE NUMERO TEL.	MENSAJES DE QUIEN? (MARCAR EXTENSION)

Malicious Call Trace language displays

Table 104: Malicious Call Trace

English	French	Italian	Spanish
MALICIOUS CALL TRACE REQUEST	DEPISTAGE D'APPELS MALVEILLANTS	RICHIESTA RINTRACCIO CHIAMATE MALEVOLE	RASTREO DE LLAMADA MALINTENCIONADA

Table continues…

English	French	Italian	Spanish
MCT activated by: for:	DAM ACTIVE par: pour:	RCM attivato da: per:	RLM activada por: para:
original call redirected from:	redirection appel initial de: (EXTENSION)	chiamata iniziale rinviata da:	llamada orig. transferida de:
party: (EXTENSION)	demandeur: (EXTENSION)	utente: (INTERNO)	usuario: (EXTENSION)
party: (ISDN SID/CNI)	demandeur: (NIP/INA ISDN)	utente: (NIC/INC ISDN)	usuario: (ISDN NIE/ INU)
party: (PORT ID)	demandeur: (REF. PORT ISDN)	utente: (ID DELLA PORTA ISDN)	usuario: (ID DEL PUERTO ISDN)
party: (ISDN PORT ID)	demandeur: (REF. PORT)	utente: (ID DELLA PORTA)	usuario: (ID DEL PUERTO)
END OF TRACE INFORMATION	FIN DES INFO DE DEPISTAGE	INFORMAZIONI FINALI SUL RINTRACCIO	FIN DE INFORMACION DE RASTREO
voice recorder port:	port enregistreur vocal:	porta del registratore:	puerto de grabado de voz:

Caller information language displays

Table 105: Caller information

English	French	Italian	Spanish
Info:	INFO.:	Info:	INFORM:

Emergency access to attendant language displays

Table 106: Emergency access to attendant

English	French	Italian	Spanish
a=xxxxxxxxxxxxxxx Ext xxxxx xx in EMRG Q	a=xxxxxxxxxxxxxxx POSTE xxxxx xx FIL URG	a=xxxxxxxxxxxxxxx Der xxxxx xx in C EMRG	a=xxxxxxxxxxxxxxx EXT xxxxx xx EN C EMRG

Queue status language displays

Table 107: Queue status

English	French	Italian	Spanish
HUNT GROUP <x> NOT ADMINISTERED	GROUPE DE DIST. <x> NON ADMINISTRE	GRUPPO <x> NON AMMINISTRATO	GRUPO BUSQUEDA <x> NO ADMINISTRADO

Queue status indication language displays

Table 108: Queue status indication

English	French	Italian	Spanish
<15 chrs> Q-time xx:xx calls xx	<15 chrs> TEMPS-F xx:xx APPELS xx	<15 chrs> T-coda xx:xx chiam xx	<15 chrs> HORA-C xx:xx LLAMADAS xx

Miscellaneous call identifier language display

Table 109: Miscellaneous call identifier

English	French	Italian	Spanish
sa (ACD Supervisor Assistance)	AS (Assistance surveillant)	as (Assistenza Supervisoree)	AS (Ayuda de supervisor)
ac (Attd Assistance Call)	AA (Appel assistance)	ao (Assistenza Operatore)	AO (Ayuda de operadora)
tc (Attd Control Of A Trunk Group)	CF (Commande faisceau)	fc (Fascio Controllato)	CE (Control enlaces)
an (Attd No Answer)	TR (Telephoniste sans reponse)	on (Operatore Non Risponde)	ON (Operadora no responde)
pc (Attd Personal Call)	AP (Appel personnel)	cp (Chiamata Personale)	LP (Llamada personal)
rc (Attd Recall Call)	RA (Rappel)	rc (Richiamata)	RL (Rellamada)
rt (Attd Return Call)	RE (Retour)	rt (Ritornata)	RT (Retorno)
sc (Attd Serial Call)	AS (Appel en serie)	ic (Inoltro a Catena)	LS (Llamada en serie)
co (Controlled Outward Restriction)	RD (Restriction de depart)	cu (Controllata Uscente)	RS (Restriccion saliente)
cs (Controlled Station to Station Restriction)	RP (Restriction vers postes)	cd (Controllata Derivati)	CS (Control estacion)
ct (Controlled Termination Restriction)	AR (Restriction d’arrivee)	ct (Controllata Terminante)	RE (Restriccion entrante)
db (DID Find Busy Station With CO Tones)	OP (Occupation du poste)	po (Passante Occupata)	EO (Estacion occupada)
da (DID Recall Go To Attd)	RT (Rappel telephoniste)	pr (Richiamata su Passante)	RD (Rellamada directa)
qf (Emerg. Queue Full Redirection)	FP (File d’urgence pleine deviation)	de (Deviata Emergenza)	DE (Desvio de emergencia)
hc (Held Call Timed Reminder)	AG (Indicatif d’appel en garde)	at (Avviso Chiamata in tenuta)	LR (Recordatorio de llamada retenida)
ic (Intercept)	IN (Interception)	in (Intercettata)	IN (Intercepcion)
ip (Interposition Call)	AI (Appel interposition)	ip (Interposizione)	EP (Entre posiciones)
ld (LDN Calls on DID Trunks)	SD (Selection directe)	pd (Diretta Passante)	LD (Larga distancia)

Table continues…

English	French	Italian	Spanish
so (Service Observing)	ES (ecoute du service)	is (Inclusione Supervisore)	SS (Supervision del servicio)
na (Unanswered or Incomplete DID Call)	SR (Sans reponse)	pn (Passante Non Risposta)	SR (Sin respuesta)
ACB (Automatic Callback)	R. AUTO. (Rappel automatique)	PRN (Prenotazione Automatica)	RA (Rellamada automatica)
callback (Callback Call)	RAPPEL (Rappel)	prenotaz (Prenotazione)	RELLAM (Rellamada)
park (Call Park)	G. I. (garde par) indicatif	parch. (Parcheggiata)	ESTAC (Estacionamiento de llamada)
control (Control)	CONTROLE (Controle)	cntr.op. (Controllo Operatore)	CONTROL (Control)
ICOM (Intercom Call)	INTERCOM (Intercommunication)	ICOM (Intercom)	INTERF (Llamda interfono)
OTQ (Outgoing Trunk Queuing)	FFD (File faisceaux de depart)	RFO (Richiamata su Fascio Occupato)	EES (Espera de enlace de salida)
priority (Priority Call)	PRIORITE (Appel prioritaire)	priorita (Priorita')	PRIORIT (Llamada prioritaria)
recall (Recall Call)	APP.RAP. (Appel rappel)	richiam (Richiamata)	REPET (Rellamada)
return (Return Call)	RETOUR (Retour)	ritorno (Chiamata Ritornata)	RETORNO (Llamada de retorno)
ARS (Automatic Route Selection)	SAA (Selection de l'acheminement automatiqe)	SAI (Selez. Autom. Instradam.)	SAR (Seleccion automatica de rutas)
forward (Call Forwarding)	RENVOI (Renvoi)	deviata (Deviata)	REENVIO (Reenvio de llamada)
cover (Cover)	SUPPL. (Suppleance)	copert. (Copertura)	COBER (Cobertura)
DND (Do Not Disturb)	NPD (Ne pas deranger)	nd (Non Disturbare)	NM (No molestar)
p (Call Pickup)	P (Prise)	a (Assente)	C (Captura de llamada)
c (Cover All Calls)	s (Suppleance)	c (Copertura)	c (Cobertura de toda llamada
n (Night Sta. Serv., Incoming No Answer)	N (Service nuit, entrant pas reponse)	n (Serv. Notte, Esterna Non Risposta)	N (Servicion noct. ext. no responde)
B (All Calls Busy)	O (Tous occupes)	O (Tutte Occupate)	O (Todas ocupadas)
f (Call Forwarding)	R (Renvoi)	d (Deviata)	R (Reenvio de llamada)
b (Cover Busy)	o (Suppleance occupee)	o (Copertura per Occupato)	o (Cobertura ocupada)
d (Cover Don't Answer)	n (Suppleance pas de reponse)	n (Copertura per Non Risposta)	n (Cobertura sin respuesta)
s (Send All Calls)	E (Envoi tous appels)	r (Rinvio)	E (Envio de toda llamada)

User identifiers language displays

Table 110: User identifiers

English	French	Italian	Spanish	Identifier
OPERATOR	TELEPHONISTE	OPERATORE	OPERADORA	Attendant
CONFERENCE	CONFERENCE	CONFERENZA	CONFERENCIA	Conference Call
EXT	POSTE	DER	EXTENSION	Extension
PAGING	PAGING	PAGING	PAGING	Paging (cannot be transplated)
OUTSIDE CALL	APPEL EXT.	ESTERNA	LLAMADA EXT.	Trunk Group
UNKNOWN NAME	INTROUVABLE	NOME SCONOSC.	DESCONOCIDO	Unknown

Property Management System interface language displays

Table 111: Property Management System interface

English	French	Italian	Spanish
CHECK IN - Ext:	ENREGISTREMENT - POSTE:	CHECK IN - Tel:	REGISTRARSE - EXTENSION:
CHECK IN: ROOM ALREADY OCCUPIED	ENREGISTREMENT: CHAMBRE OCCUPEE	CHECK IN: CAMERA OCCUPATA	REGISTRARSE: HABITACION OCUPADA
CHECK IN COMPLETE	ENREGISTREMENT EFFECTUE	CHECK IN COMPLETATO	REGISTRO TERMINADO
CHECK IN FAILED	ECHEC D'ENREGISTREMENT	CHECK IN ERRATO	REGISTRARSE: FALLIDO
CHECK OUT - Ext:	DEPART - POSTE:	CHECK OUT - Tel:	PAGAR LA CUENTA - EXTENSION:
CHECK OUT COMPLETE: MESSAGE LAMP OFF	DEPART: PAS DE MESSAGES	CHECK OUT COMPLETATO: NESSUN MESSAGGIO	PAGO TERMINADO: NINGUN MENSAJE
CHECK OUT COMPLETE: MESSAGE LAMP ON	DEPART: MESSAGES	CHECK OUT COMPLETATO: MESSAGGI IN ATTESA	PAGO DE CUENTA TERMINADO: MENSAJES
CHECK OUT FAILED	ECHEC PROCEDURE DE DEPART	CHECK OUT ERRATO	PAGAR LA CUENTA: FALLIDO
CHECK OUT: ROOM ALREADY VACANT	DEPART - CHAMBRE INOCCUPEE	CHECK OUT: CAMERA NON OCCUPATA	PAGAR LA CUENTA: HABITACION VACANTE
MESSAGE LAMP OFF	PAS DE MESSAGES	NESSUN MESSAGGIO IN ATTESA	LUZ DE MENSAJE APAGADA
MESSAGE LAMP ON	MESSAGES	MESSAGGI IN ATTESA	LUZ DE MENSAJE ENCENDIDA

Table continues…

English	French	Italian	Spanish
MESSAGE NOTIFICATION FAILED	ECHEC D'AVIS MESSAGES	NOTIFICA MESSAGGI ERRATA	AVISO DE MENSAJE FALLIDO
MESSAGE NOTIFICATION OFF - Ext: xxxxx	AVIS DE MESSAGES DESACTIVE - POSTE:xxxxx	NOTIFICA MESSAGGI DISABIL. - Tel: xxxxx	AVISO DE MENSAJE APAGADO - EXT: xxxxx
MESSAGE NOTIFICATION ON - Ext: xxxxx	AVIS DE MESSAGES ACTIVE - POSTE:xxxxx	NOTIFICA MESSAGGI ABILITATA - Tel: xxxxx	AVISO DE MENSAJE ENCENDIDO - EXT: xxxxx

Security Violation Notification language displays

Table 112: Security Violation Notification

English	French	Italian	Spanish
Barrier Code Violation	VIOLATION DU CODE D'ENTREE	VIOLAZIONE DI CODICI DE TAGLIO	VIOLACIAON CONDIGO LIMITE
Login Violation	VIOLATION DE L'ACCES A L'ADMINISTRATION	IOLAZIONE DI INIZIO DI REGISTRAZIONE	VIOLACION CLAVE ACCESO
Station Security Code Violation	VIOLATION DE CODE D'ACCESS DE SECURITE	VIOLAZIONE DI CODICE DE SICUREZZA UTENTE	VIOLACION DE SEGURIDAD DE LA ESTACION
Authorization Code Violation	VIOLATION DEU CODE ACCES	VIOLAZION DEL CODICE D'AUTHORIZZAZIONE	VIOLACION DE CODIGO DE AUTORIZACION

Stored number language displays

Table 113: Stored number

English	French	Italian	Spanish
NO NUMBER STORED	AUCUN NUMERO EN MEMOIRE	NESSUN NUMERO IN MEMORIA	NINGUN NUMERO ALMACENADO

Special codes language displays

Table 114: Special codes

English	French	Italian	Spanish
m (Mark)	M (Marquer)	m (Marcato)	M (Marca)
p (Pause)	P (Pause)	p (Pausa)	P (Pausa)
s (Suppress)	S (Supprimer)	s (Soppresso)	S (Suprimir)
w (Wait)	A (Attendre)	a (Attesa)	E (Espera)
W (Indefinite Wait)	a (Attendre)	A (Attesa)	e (Espera)

Station Hunting language displays

Table 115: Calling party display

English	French	Italian	Spanish
HUNT	Routage	Ricerca	Busqueda

Table 116: Hunt-to station display

English	French	Italian	Spanish
h	r	r	b

Time-of-Day routing messages language displays

In these displays, x and y denote the Route Plan Number (RPN 1-8), yyy is a 3-letter abbreviation for the day of the week, and zz:zz is the activation time (24-hour time).

Table 117: Time-of-Day routing messages

English	French	Italian	Spanish
ENTER ACTIVATION ROUTE PLAN, DAY & TIME	ENTRER PLAN D'ACTIVATION, JOUR ET HEURE	INTRODURRE PIANO DA ATTIV., GIORNO E ORA	INTRODUZCA PLAN ACT DE RUTAS, DIA Y HORA
ENTER DEACTIVATION DAY AND TIME	ENTRER JOUR ET HEURE DE DESACTIVATION	INTRODURRE GIORNO E ORA DI DISATTIVAZ	INTRODUZCA DIA Y HORA DE DESACTIVACION
OLD ROUTE PLAN: x ENTER NEW PLAN:	ACHEMINEMENT ANT.: x ENTRER NOUVEAU:	INSTRADAMENTO PREC: x INTROD IL NUOVO:	PLAN RUTAS ANT: x INTRODUZCA EL NUEVO:
OLD ROUTE PLAN: x NEW PLAN: y	ACHEMINEMENT ANT.: x NOUVEAU PLAN: y	INSTRADAMENTO PREC: x NUOVO PIANO: y	PLAN RUTAS ANT: x NUEVO PLAN: y
ROUTE PLAN: x FOR yyy ACT-TIME: zz:zz	ACHEM.: x POUR yyy ACT-HEURE: zz:zz	INSTRADAMENTO: x PER yyy ATTIV ORE:zz:zz	PLAN RUTAS: x PARA yyy HORA-ACT: zz:zz
ROUTE PLAN: x FOR yyy DEACT-TIME: zz:zz	ACHEM.: x POUR yyy DESACT-HEURE: zz:zz	INSTRADAM.: x PER yyy DISATTIV ORE:zz:zz	PLAN RUTAS: x PARA yyy HORA-DESACT:zz:zz

Time-of-Day routing days of the week language displays

This table lists the 3-letter abbreviations for the day of the week.

Table 118: Time-of-Day routing days of the week

English	French	Italian	Spanish
MON	LUN	LUN	LUN

Table continues…

English	French	Italian	Spanish
TUE	MAR	MAR	MAR
WED	MER	MER	MIE
THU	JEU	GIO	JUE
FRI	VEN	VEN	VIE
SAT	SAM	SAB	SAB
SUN	DIM	DOM	DOM

Transfer completed language displays

English	French	Italian	Spanish
TRANSFER COMPLETED	TRANSFERT EFFECTU	TRASFERIMENTO COMPLETATO	TRANSFERENCIA REALIZADA

Mapping enhanced display characters

Use the following tables to map US English characters to Russian, Japanese, European, or Ukrainian characters. The terminal displays the characters in the order in which you enter them. If you want the display to read right to left, enter the characters in reverse order on the screen.

US English to Russian characters

US English to Russian characters

Russian	US English	Russian	US English
space	space	Й	Q
Ф	A	К	R
И	B	Ы	S
С	C	Е	T
В	D	Г	U
У	E	М	V
А	F	Ц	W
П	G	Ч	X
Р	H	Н	Y
Ш	I	Я	Z
О	J	Х	[
Л	K	Ъ	]
Д	L	Ж	;
Ь	M	э	\
Т	N	Б	,
Щ	O	Ю	.
З	P		

US English to Japanese characters

Japanese	US English	Japanese	US English
space	space	ｺ	:
｡	!	ｻ	;
｢	“	ｼ	<
｣	#	ｽ	=
､	$	ｾ	>
･	%	ｿ	?
ｦ	&	ﾀ	@
ｧ	‘	ﾁ	A
ｨ	(	ﾂ	B
ｩ	)	ﾃ	C
ｪ	*	ﾄ	D
ｫ	+	ﾅ	E
ｬ	,	ﾆ	F
ｭ	-	ﾇ	G
ｮ	.	ﾈ	H
ｯ	/	ﾉ	I
ｰ	0	ﾊ	J
ｱ	1	ﾋ	K
ｲ	2	ﾌ	L
ｳ	3	ﾍ	M
ｴ	4	ﾎ	N
ｵ	5	ﾏ	O
ｶ	6	ﾐ	P
ｷ	7	ﾑ	Q

Japanese	US English	Japanese	US English
ｦ	8	ｲ	R
ｧ	9	ｴ	S
ｨ	[	ｳ	T
ｩ	\	ｵ	U
ｪ	]	ｶ	V
	^	ｷ	W
ｫ	_	ｸ	X
		ｹ	Y
		ｺ	Z

For Japanese, the letter z and the left brace { and the pipe (|) characters map to Kanji characters as follows:

- The letter z. Symbol for 1,000
- The left brace {. Symbol for 10,000
- The pipe (|). Symbol for Yen

US English to European characters

The following map displays some of the characters in only uppercase or lowercase, such as, €, Ê, ø, and others.

European	US English	European	US English
í	space	ø	=
ï	!	æ	>
ã	“	Ó	?
á	#	î	@
à	$	å	A
ú	%	ą	B
ù	&	â	C
é	‘	ű	D
è	(	ů	E
ć	)	è	F
ł	*	ė	G
Ď	+	ę	H
ý	,	Ç	I
ž	-	ř	J
õ	.	Đ	K
ò	/	ÿ	L
Í	0	ń	M
Ï	1	Æ	N
Ã	2	ő	O
Á	3	Î	P
À	4	Å	Q
Ú	5	Ă	R

European	US English	European	US English
Ù	6	Â	S
É	7	Ü	T
È	8	Ů	U
č	9	Ê	V
Ł	:	ë	W
đ	;	Ę	X
Ý	<	ś	Y
ř	Z	â	z
´	[	Ă	s
Ÿ	\	ū	t
Ń	]	Ō	u
Ň	^	Ě	v
ō	_	Ë	w
ì	`	ğ	x
ä	a	Ş	y
β	b	Ť	z
ú	d	þ	{
Ü	e	Ż	|
ě	f	Ň	}
ë	g		
ğ	h		
š	i		
Ţ	j		
¿	k		
ź	l		
ń	m		
ñ	n		
ö	o		
İ	p		
Ă	q		

US English to Ukrainian characters

Ukrainian	US English	Ukrainian	US English
space	space	й	Q
Ф	A	К	R
И	B	;	S
С	C	Е	T
В	D	г	U
У	E	М	V
А	F	Ц	W
П	G	ч	X
Р	H	Н	Y
Ш	I	Я	Z
О	J	Х	[
Л	K	І	]
д	L	Ж	;
ь	M	Є	\
Т	N	Б	,
Щ	O	ю	.
З	P		

Telephone Display administration

This section describes the screens that you use to administer the Telephone Display feature.

Screens for administering Telephone Display

Screen name	Purpose	Fields
Date/Time Mode and Formats - English	Set up the appearance of the date and time displays.	All
Date/Time Mode and Formats - French, Italian, Spanish, User-Defined, and Unicode	Set up the appearance of the date and time displays.	All

Table continues…

Screen name	Purpose	Fields
Language Translations	Enter translations in a user-defined language.	All
Leave Word Calling Format - English	Set up the appearance of the Leave Word Calling displays.	All
Leave Word Calling Format - French, Italian, Spanish, User-Defined, and Unicode	Set up the appearance of the Leave Word Calling displays.	All

Interactions for Telephone Display

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

The following interactions apply to all capabilities:

- Distributed Communications System

  Trunk group and attendant information that is associated with a Distributed Communications System (DCS) call can be translated. If the displays are disassociated with a DCS call, the system displays the name the trunk group that is administered on the Trunk Group screen.
- Single-Digit Dialing and Mixed-Station Numbering

  If the system dial plan uses prefixed extensions, the prefix is not displayed when the extension is displayed. Users can use the Return Call button to dial prefixed extensions, because the system dials the prefix, even though the prefix is not displayed.

The following interactions pertain to the Enhanced Telephone Display capability:

- Adjunct Switch Application Interface (ASAI) and related adjuncts

  Information that Communication Manager sends to any adjunct is the literal value of the field, not the enhanced characters. The system displays a string of random characters. For example, “2<@^.”
- INTUITY AUDIX Voice Power and Audix Voice Power Lodging

  Not supported.
- Data Call Setup

  Not supported.
- Distributed Communications Systems (DCS)

  All switch nodes in a DCS network must have must have the same software load installed on each server or media server, must have the enhanced characters enabled, and must have telephones with the same firmware type.
- ECMA and QSIG Networking

  Information must be sent between the servers that run Communication Manager.

- Leave Word Calling - Adjunct

  Not supported.

- Message Retrieval - Print Messages (Demand Print)

  Not supported.

- Monitor 1 and OneVision

  Monitor 1 and OneVision receive ASCII characters.

- OSSI

  OSSI displays the literal value of the display field, and not the enhanced characters.

- Passageway Direct Connect

  Not supported.

- VUStats

  You must use telephones that support enhanced characters. If telephones do not use enhanced characters, the software might clear the display, or show the information on the display incorrectly.

Chapter 178: Temporary Bridged Appearance

With the Temporary Bridged Appearance feature, extension to cellular users and multiappearance telephone users in a Terminating Extension Group (TEG) or a Personal Central Office Line (PCOL) group can bridge on an existing group call. If the Call Pickup feature is used to answer the call, the originally called party can bridge onto the call. The called party can use this feature to bridge onto a call that redirects to coverage before the called party can answer the call.

Detailed description of Temporary Bridged Appearance

An incoming call to a Terminating Extension Group (TEG) or Private Central Office Line (PCOL) group is not a call to an individual. However, one particular member of the group can be the most qualified person to handle the given call. If this individual does not answer the call originally, this individual can bridge onto the call. The answering party does not have to transfer the call.

A call to an individual can be answered by a member of a call pickup group. While the call is still connected, the called party can bridge onto the call, and the answering party hangs up.

Call Coverage provides redirection of calls to alternate answering positions or covering users. A temporary bridged appearance is maintained at the called telephone.

The called party can answer the call at any time, even if the call is already answered by a covering user. If the called party does not bridge onto the call, the covering user can use the Consult function of Call Coverage to determine if the called party wants to accept the call. The Consult function uses the temporary bridged appearance that is maintained on the call. When the consult call is finished, the temporary bridged appearance is removed.

Stations that usually have a temporary bridged appearance with their coverage point do not have a temporary bridged appearance if the coverage point is Communication Manager Messaging.

Temporary Bridged Appearance administration

This section describes the screens that you use to administer the Temporary Bridged Appearance feature.

Screens for administering Temporary Bridged Appearance

Screen name	Purpose	Fields
Feature-Related System Parameters	Enable the Temporary Bridged Appearance feature for Call Pickup.	Temporary Bridged Appearance on Call Pickup
system-parameters coverage-forwarding	Govern how a covering user who has placed an answered coverage call on hold is treated if the original principal bridges onto the call.	Keep Held SBA at Coverage Point
	Allow a user to maintain a simulated bridged appearance when a call redirects to coverage.	Maintain SBA At Principal
	Either direct the system to maintain a simulated bridged appearance on the principal when redirecting to a final off-net coverage point or allow the system to drop the SBA on the principal's telephone when the call redirects off-net at the last coverage point, eliminating the cut-through delay inherent in CCRON calls, but sacrificing the principal's ability to answer the call.	Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point

Considerations for Temporary Bridged Appearance

This section provides information about how the Temporary Bridged Appearance feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Temporary Bridged Appearance under all conditions. The following considerations apply to Temporary Bridged Appearance:

- With Temporary Bridged Appearance, a party can bridge onto a call. The answering party does not have to transfer the call, which is convenient and saves time.
- Temporary Bridged Appearance does not provide the capability to originate calls, or the capability to answer the calls of another party. The Bridged Call Appearance feature provides these capabilities.
- If two parties are bridged together on an active call with a third party, and if the Conference Tone feature is enabled, conference tone is heard.
- The Bridged Call Appearance feature enhances Temporary Bridged Appearance by allowing:
  - More than one call to an extension to be bridged.
  - Calls to be originated from bridged appearances.

Interactions for Temporary Bridged Appearance

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

Call Coverage

Calls that are redirected to Call Coverage maintain a temporary bridged appearance on the called telephone if a call appearance is available to handle the call. The called party can bridge onto the call at any time. You can administer the system to allow a temporary bridged appearance of the call to either remain at, or be removed from, the covering telephone after the principal bridges onto the call. If two parties are bridged together on an active call with a third party, all three parties hear the bridging tone.

Consult

Consult calls use the temporary bridged appearance that is maintained on the call. At the conclusion of a consult call, the bridged appearance is no longer maintained. If the principal chooses not to talk with the calling party, the principal cannot bridge onto the call later.

Conference and Transfer

If a call has, or had a temporary bridged appearance and the call is then conferenced or transferred, and is redirected to coverage again, a temporary bridged appearance is not maintained at the conferenced-to or the transferred-to extension.

Privacy - Manual Exclusion

When Privacy - Manual Exclusion is activated, other users are prevented from bridging onto a call. A user who attempts to bridge onto a call when this feature is active is dropped.

Note:

The displays of IP telephones and call logs show whether calls were answered through call pickup from another station, and if the Temporary Bridged Appearance feature is in use. This does not apply to pickup through the Team button.

Chapter 179: Tenant Partitioning

Use the Tenant Partitioning feature to provide telecommunications services to multiple independent groups of users through a single server that runs Communication Manager. The Tenant Partitioning feature usually provides these services from a single provider to multiple tenants of an office complex. Each tenant seems to have a dedicated Communication Manager, even though the tenants share the same Communication Manager. You can also use this feature to provide group services, such as departmental attendants, on a single-customer server that runs Communication Manager.

Detailed description of Tenant Partitioning

The Tenant Partitioning feature is unavailable with Offer B.

The Tenant Partitioning feature provides the following services to tenants:

- Telephone equipment
- Building wiring
- Public network access and private network access
- Attendant services

You can also use the Tenant Partitioning feature to assign a separate music source to each tenant partition that plays when a user or an attendant places a caller on hold.

Note:

If you use equipment that rebroadcasts music or other copyrighted materials, you might be required to obtain a copyright license from, or pay fees to, a third party. A Magic-on-Hold system does not require such a license. You can purchase a Magic-on-Hold system from Avaya, or from an Avaya business partner.

Proper administration can protect tenant resources, including trunking facilities, and all other Communication Manager endpoints from unauthorized access by other tenants.

For the Tenant Partitioning feature to function properly in your system, you must ensure that:

- All tenants can call and be called by tenant 1. This is the system default. If you change this default, some call types fail. For example, dial 0 fails, as do security violation calls and automatic circuit assurance calls.

- All stations in a call-pickup group are under control of the same tenant.
- All stations with bridged appearances are under control of the same tenant.
- Stations in different departments, for the purposes of attendant services, can call each other.

You must assign a tenant partition number to each entity, such as an endpoint or a virtual endpoint, to which you assign a Class of Restriction (COR). You do not assign a tenant partition number to an authorization code or to fixed-assignment virtual endpoints.

You must specify an attendant group for each tenant that you define, even if the attendant group does not have an assigned console. You must also assign an attendant console to a tenant partition, and you must assign a group number to the attendant console.

Guidelines for partitioning tenants

The system has a default of one universal tenant for the system. This tenant is in partition 1, and is usually the service provider. Another system default that the tenant in partition 1 has access to all facilities in the system, and that all other tenants can access the tenant in partition 1. The tenant in partition one is usually referred to as tenant 1.

The service provider creates additional partitions that are based on tenant requirements. When you create tenant partitions, remember that:

- You can assign each Communication Manager endpoint to only one tenant partition. And, you must pass each endpoint to a partition. For example, you must assign each telephone, attendant console, trunk, and virtual endpoint. Virtual endpoints include listed directory numbers and virtual directory number (VDN) to a tenant partition.
- Most tenant partitions are separate units. By default, the system does not allow tenants, except tenant 1, to access telephones or trunk facilities that belong to other tenants. However, you can change this system default. You can give explicit permission for a tenant to access another tenant. For example, you can allow tenant 6 to call only tenant 9 and tenant 16.

  Note:

  If a tenant has permission to call another tenant, the tenant has access to all the endpoints that belong to the other tenant. For example, if tenant 6 has permission to call tenant 9, tenant 6 can also use any trunk facilities in tenant partition 9.
- The system can use tenant partitioning restrictions to block calls between two users in the system. However, either user can use the Direct Inward Dialing (DID) extension of the other user to call over the public network.
- If tenants want to share some, but not all, facilities, you must group the shared facilities into a separate partition. For example, if two tenants share a trunk, but do not have direct system access to call each other, put the trunk in its own partition. Both tenants can then access the trunk.

You must also consider the constraints and the requirements of access control, attendant services, music sources on hold, and network route selection when you establish or assign partitions.

Access control with Tenant Partitioning

Tenant-to-tenant access restrictions limit some features, such as Call Coverage. For example, the coverage of tenant 2 includes a telephone from tenant 3 in its coverage path. If tenant 4 has permission to call tenant 2, but does not have permission to call tenant 3, a call from tenant 4 to tenant 2 skips the tenant 3 coverage point.

You might also want to set up tenants with special access privileges. For example, you might give a restaurant in an office complex permission to receive calls from any other tenant. You might also want tenants to have permission to call, or be called by, building security, or those who administer and troubleshoot Communication Manager.

You can also assign all central office (CO) trunks to one tenant partition. All other tenants can then access the CO trunks.

Attendant services with Tenant Partitioning

With Tenant Partitioning, you can administer personalized attendant services for each tenant.

The system provides one principal attendant, and either one night attendant or one day and night attendant, for each attendant group. You assign each tenant an attendant group for service. Each attendant group has a separate queue. Queue warning lamps remain dark when Tenant Partitioning is active. However, when someone presses a queue-status button, the system displays the status of the attendant-group queue. The total number of calls queued for all tenants cannot exceed the system limit.

Attendant groups can serve more than one tenant, if the two tenants have permission to access each others facilities. For example, can use the facilities of one tenant to extend a call to another tenant, if the tenant has permission to access the facilities of the other tenant.

Each tenant can have a designated night-service station. When a night attendant is unavailable, the system directs calls to an attendant group that is in night service, to the night-service station of the appropriate tenant. When someone places an attendant group into night service, all trunk groups and hunt groups that belong to tenants that the attendant group serves, go into night service. In this case, the system routes incoming calls to the night-service destination of the appropriate tenant. Each tenant can have exclusive access to the following entities:

- Listed directory number (LDN) night destination
- Trunk answer on any station (TAAS) port
- Night attendant

An attendant can specify that access to a trunk group is under attendant control, if the trunk group is assigned to a tenant served by that attendant group. The system directs any valid user attempt to access the trunk group to the attendant group that serves the tenant.

Network route selection with Tenant Partitioning

You can place trunk groups that belong to different tenants in the same route pattern. Calls that the system routes to that pattern select the first trunk group in the pattern that has caller access permission.

Tenant Partitioning examples

The following example describes how you might administer Tenant Partitioning in an office complex.

You assign tenant partition 1, the universal tenant, as the service provider. All other tenants can call, and be called by, the service provider.

You assign tenant partitions 2 through 15 to individual businesses in the complex. You maintain the system-default restrictions for these tenants. These restrictions specify that tenants cannot access the telephones, the trunk facilities, or the other Communication Manager endpoints that belong to other tenants.

You assign tenant partition 16 to the restaurant in the building complex. You give all tenants permission to call the restaurant. However, to prevent access to trunks and other facilities that belong to other tenants, you do not allow the restaurant to call the other tenants.

You assign tenant partition 17 to all the CO trunk groups. You give all tenants permission to call tenant 17.

You assign tenant partition 18 to a trunk group that tenants 3 and 7 want to share. You give tenants 3 and 7 access to this partition, and you deny all other tenants access to partition 18. To prevent toll fraud, you do not allow tenant 18 to place calls to tenant 18.

All tenants can use the same Automatic Route Selection (ARS) route pattern. In this example, the trunk for tenant partition 18, the private trunk that tenants 3 and 7 share, is first in the route pattern. Tenant partition 17 is second in the route pattern. The system routes calls that tenants 3 and 7 make to partition 18 and then, as a second option, to partition 17. The system routes all other tenants directly to partition 17, because you deny all other tenants access to partition 18.

Assign the facilities that the tenants do not share to the tenant partition that the facilities serve. These facilities can include trunk groups, VDNs, telephones, attendant consoles, and other endpoints.

The table on page 1344 summarizes the calling permissions for the different tenant partitions. “Yes” indicates that the partitions have permission to call, and be called by, each other. “No” indicates that partitions cannot call, or be called by, each other.

Table 119: Calling permissions for the partitions

Calling tenant partition number	Called tenant partition number					
	1	2, 4 through 6, and 8 through 15	3, 7	16	17	18
1	Yes	Yes	Yes	Yes	Yes	Yes
2, 4-6, 8-15	Yes	Each partition can call itself, but cannot call the other partitions.	No	Yes	Yes	No

Table continues…

Calling tenant partition number	Called tenant partition number					
	1	2, 4 through 6, and 8 through 15	3, 7	16	17	18
3, 7	Yes	No	Each partition can call itself, but cannot call the other partitions.	Yes	Yes	Yes
16	Yes	No	No	Yes	Yes	No
17	Yes	Yes	Yes	Yes	Yes	No
18	Yes	No	Yes	No	No	No

Multiple Music-on-Hold with Tenant Partitioning

Using Tenant Partitioning, you can assign a separate music source to each tenant partition. A caller hears the music when a user places a call on hold. The tenant number that you assign to the called extension usually determines the music source that the user hears. With this capability, you can customize the music, or the messages, for the business needs of each tenant partition.

If the COR of the user extension that places the call on hold supports music-on-hold, a caller on hold hears the music source that is assigned to the partition at which the call initially terminates. For example, if the system first routes a call to an Communication Manager Messaging automated attendant, and then routes the call to the appropriate tenant partition, the caller who is on hold hears the music source of the Communication Manager Messaging automated attendant. The caller who is on hold does not hear the music source of the tenant partition to which the system routes the call. Likewise, if a caller in tenant partition 2 makes an out-going call that uses the trunk groups of tenant 3, the caller hears the music source that is assigned to tenant 3. If the COR of the called extension does not support music on hold, the caller hears nothing.

The maximum number of allowed music sources is the same as the maximum number of allowed tenant partitions. More than one tenant partition can use each music source.

The table on page 1345 shows which music-on-hold types that you can assign to each tenant partition.

Table 120: Types of music-on-hold

Type	System response for a call who is on hold
none	Silence
tone	System-wide administered tone
music	This is the type of music that is associated with the administered port. The number of allowed music sources equals the number of allowed tenant partitions. Each partition can have its own music source.

Tenant Partitioning administration

The following tasks are part of the administration process for the Tenant Partitioning feature:

- Defining a tenant partition
- Assigning a tenant partition number to an access telephone
- Assigning a tenant partition number to an agent login ID
- Assigning a tenant partition number to an announcement
- Assigning a tenant partition number to an attendant
- Assigning a tenant partition number to a data module
- Assigning a tenant partition number to a hunt group
- Assigning a tenant partition number to a loudspeaker paging zone
- Assigning a tenant partition number to The remote access extension
- Assigning a tenant partition number to a user extension
- Assigning a tenant partition number to a terminating extension group
- Assigning a tenant partition number to a trunk group
- Assigning a tenant partition number to a vector directory number
- Assigning the sources of music for the tenant partitions

Related links

Defining a tenant partition on page 1348
Assigning a tenant partition number to an access telephone on page 1349
Assigning a tenant partition number to an agent login ID on page 1349
Assigning a tenant partition number to an announcement on page 1349
Assigning a tenant partition number to an attendant on page 1350
Assigning a tenant partition number to a data module on page 1350
Assigning a tenant partition number to a hunt group on page 1350
Assigning a tenant partition number to a loudspeaker paging zone on page 1350
Assigning a tenant partition number to the remote access extension on page 1350
Assigning a tenant partition number to a user extension on page 1351
Assigning a tenant partition number to a terminating extension group on page 1351
Assigning a tenant partition number to a trunk group on page 1351
Assigning a tenant partition number to a vector directory number on page 1351
Assigning the sources of music for the tenant partitions on page 1351

Preparing to administer Tenant Partitioning

Procedure

Ensure that the **Tenant Partitioning** field on the Optional Features screen is set to y.

If the **Tenant Partitioning** field is set to n, your system does not support the Tenant Partitioning feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Tenant Partitioning, or to open a service request.

To view the Optional Features screen, enter `display system-parameters customer-options`.

Screens for administering Tenant Partitioning

Screen name	Purpose	Fields
Access Endpoint	Assign a tenant partition number to an access endpoint.	TN
Agent LoginID	Assign a tenant partition number to an agent login ID.	TN
Announcements/Audio Sources	Assign a tenant partition number to an announcement that is assigned to an extension.	TN
Attendant Console	Assign the group number and the tenant partition number to an attendant.	• Group • TN
Data Module	Assign a tenant partition number to a data module.	TN
Feature-Related System Parameters	Enable the Tenant Partitioning feature for your system.	Tenant Partitioning
Hunt Group	Assign a tenant partition number to a hunt group.	TN
Loudspeaker Paging	Assign a tenant partition number to each loudspeaker paging zone.	TN
Music Sources	Assign the sources of the music for the system.	All
Remote Access	Assign a tenant partition number to the remote access extension.	TN
Station	Assign a tenant partition number to a user extension.	TN
Tenant	Define a tenant to the system.	All
Terminating Extension Group	Assign a tenant partition number to a Terminating Extension Group (TEG).	TN
Trunk Groups	Assign a tenant partition number to a trunk group.	TN
Vector Directory Number	Assign a tenant partition number to a vector directory number (VDN).	TN

Defining a tenant partition

Procedure

1. Enter `change tenant n`, where *n* is the tenant that you want to change.

   The **Tenant** field is a display-only field. This field contains the tenant number that you typed on the command line.

2. In the **Tenant Description** field, type a description of the tenant.

   You can type 40 characters. You can leave the field blank, but a description helps you identify the tenant when you change other information about the tenant.

3. In the **Attendant Group** field, type the number of the attendant group for the tenant partition.

   The system assigns the number 1 as the default for the **Attendant Group** field.

   The default for the system is that all attendant groups exist. However, the attendant group is empty if you do not assign consoles to the attendant group.

4. In the **Ext Alert Port (TAAS)** field, perform one of the following actions:

   - If trunk answer from any station (TASS) alert port information does not exist, type an `x`.
   - If TASS alert port information exists, enter the 7-character port number.

     The media module must be installed and defined to the system before you can refer to the media module in the **Ext Alert Port (TAAS)** field. The port type and the object type must be consistent. You can assign the port to only one tenant.

     Table 121: Port information for the Ext Alert Port (TAAS) field

Characters	Description	Value
1-3	Gateway number	G4xx Media Gateway Number
4	Gateway	V
5	Slot number	1 through 8
6-7	Circuit number	Port number on media module

5. In the **Night Destination** field, type the night service station extension, if you want night service for the tenant.

   Type an extension that already exists in the system.

6. In the **Ext Alert (TAAS) Extension** field, type an extension that already exists in the system.

   Note that, the system displays the **Ext Alert (TAAS) Extension** field if you type an `x` in the **Ext Alert Port (TAAS)** field.

7. In the **Music** field, type the source of the music or the tone for the tenant partition.
8. Select **Enter** to save your changes.
9. Click **Next** until you see the **Calling Permission** area.

Note:

The **Tenant** field is a display only field. This field contains the tenant number that you entered on the command line.

10. In the numbered fields, perform one of the following actions:
    - To enable calling permission between the tenant that you entered in the command line and any other tenant in the system, type `y`.
    - To disable calling permission between the tenant that you entered in the command line and any other tenant in the system, type `n`.

    The system default for the calling permissions are to:

    - Allow the tenant to call itself
    - Allow the tenant to call tenant 1
    - Turn off all other calling permissions between tenants

Assigning a tenant partition number to an access telephone

Procedure

1. Enter `change access-endpoint n`, where *n* is the extension of the access telephone.
2. In the **TN** field, type the tenant partition number for the access endpoint.
3. Select **Enter** to save your changes.

Assigning a tenant partition number to an agent login ID

Procedure

1. Enter `change agent loginid n`, where *n* is the number of the agent login ID that you want to change.
2. In the **TN** field, type the tenant partition number for the agent login ID.

   The system assigns the number 1 as the default for a tenant partition number.
3. Select **Enter** to save your changes.

Assigning a tenant partition number to an announcement

Procedure

1. Enter `change announcements`.
2. In the **TN** field, type the tenant partition number for the extension.

   The system assigns the number 1 as the default for a tenant partition number.
3. Select **Enter** to save your changes.

Assigning a tenant partition number to an attendant

Procedure

1. Enter `change attendant n`, where *n* is the number of the attendant that you want to change.
2. In the **Group** field, type the group number for the Attendant.
3. In the **TN** field, type the tenant partition number for the Attendant.
4. Select **Enter** to save your changes.

Assigning a tenant partition number to a data module

Procedure

1. Enter `change data-module n`, where *n* is the extension of the data module.
2. In the **TN** field, type the tenant partition number for the data module.
3. Select **Enter** to save your changes.

Assigning a tenant partition number to a hunt group

Procedure

1. Enter `change hunt-group n`, where *n* is the hunt group number to which you want to assign a partition number.
2. In the **TN** field, type the tenant partition number for the hunt group.
3. Select **Enter** to save your changes.

Assigning a tenant partition number to a loudspeaker paging zone

Procedure

1. Enter `change paging loudspeaker`.
2. In the **TN** field, type the tenant partition number for the loudspeaker paging zone.
3. Select **Enter** to save your changes.

Assigning a tenant partition number to the remote access extension

Procedure

1. Enter `change remote-access`.
2. In the **TN** field, type the tenant partition number for the remote access extension.

   The system assigns the number 1 as the default tenant partition number.
3. Select **Enter** to save your changes.

Assigning a tenant partition number to a user extension

Procedure

1. Enter `change station n`, where *n* is the extension to which you want to assign a tenant partition number.
2. In the **TN** field, type the tenant partition number for the user extension.
3. Select **Enter** to save your changes.

Assigning a tenant partition number to a terminating extension group

Procedure

1. Enter `change term-ext-group n`, where *n* is the terminating extension group number to which you want to assign a tenant partition number.
2. In the **TN** field, type the tenant partition number for the TEG.

   The system assigns the number 1 as the default for a tenant partition number.
3. Select **Enter** to save your changes.

Assigning a tenant partition number to a trunk group

Procedure

1. Enter `change trunk-group n`, where *n* is the trunk group number to which you want to assign a tenant partition number.
2. In the **TN** field, type the tenant partition number for the trunk group.
3. Select **Enter** to save your changes.

Assigning a tenant partition number to a vector directory number

Procedure

1. Enter `change vdn n`, where *n* is the VDN to which you want to assign a tenant partition number.
2. In the **TN** field, type the tenant partition number for the VDN.
3. Select **Enter** to save your changes.

Assigning the sources of music for the tenant partitions

Procedure

1. Enter `change music-sources`.

   The **Source** field is a display-only field.

   - Note that if the **Tenant Partitioning** field on the Optional Features screen is set to y:

The Feature-Related System Parameters screen does not display the **Music/Tone on Hold** field.

The first **Source** field on the Music Sources screen displays the value in the **Music/Tone on Hold** field on the Feature-Related System Parameters screen.

If the value in the **Music/Tone on Hold** field on the Feature-Related System Parameters screen contained music, the Music Sources screen also displays the port address.

- Note that if the **Tenant Partitioning** field on the Optional Features screen is set to n:

The **Music/Tone on Hold** field reappears on the Feature-Related System Parameters screen.

The system displays the value from the Music Sources screen, in the **Music/Tone on Hold** field on the Feature-Related System Parameters screen.

2. In the **Type** field, perform one of the following actions:
   - If you want the users to hear music, type `music`.
   - If you want the users to hear the tone-on-hold tone, type `tone`.

     You can specify tone for only one music source.
   - If you want the users to hear nothing, type `tone`.
3. In the **Port** field, type the auxiliary trunk address or the analog port address of the music source.

   You cannot enter duplicate addresses in the **Port** field.

   The system displays the Port field only if you typed music in the **Type** field.
4. In the **Description** field, type a maximum of 20 characters that describe the source of the music.

   The system displays the Description field, only if you typed music or tone in the **Type** field.
5. Select **Enter** to save your changes.

Interactions for Tenant Partitioning

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

Tenant-partition identification is not passed between servers. A network of servers that run Communication Manager does not enforce Tenant Partitioning restrictions without special administration. For example, Tenant Partitioning on a network of servers that run Communication Manager does not enforce tenant-specific tie trunks.

Administration of the following features requires special care to avoid unintended access between tenants.

- Bridging
- Call Pickup
- Call Vectoring
- Controlled Restriction
- Facility Busy Indication
- Facility Test Calls
- Integrated Directory
- Inter-PBX Attendant Calls
- Main/Satellite/Tributary
- Malicious Call Trace
- Personal central office (CO) line
- Private Networking - Automatic Alternate Routing (AAR)
- Service Observing
- Uniform Dial Plan

Specific information about how the Tenant Partitioning feature interacts with other features follows.

Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS)

The Tenant Partitioning feature is not the same as the Time-of-Day Plan Numbers or the Partition Groups in AAR and ARS.

However, if you use the Tenant Partitioning feature, you can use the Time-of-Day Plan Numbers and the Partition Groups in AAR and ARS.

Attendant and Attendant Group features

The Tenant Partitioning feature creates multiple attendant groups. Attendant operations such as direct-station or direct trunk group select (DTGS) are subject to tenant-to-tenant restrictions, both at selection time and at split time.

All the calls that an attendant within an attendant group places on hold hear the music source from the attendant group.

Attendant Control of Trunk Group Access

An attendant group controls access to the trunk groups of the tenants that the attendant group serves. An attendant does not control access to any other trunk groups.

Communication Manager Messaging

The system applies the same tenant-to-tenant restrictions to Communication Manager Messaging voice and data ports that the system applies to any other endpoints.

Communication Manager Messaging can restrict one group of subscribers from sending voice mail to another tenant partition group.

Those who control the tenant partitions can:

- Create 10 different communities within each Communication Manager Messaging
- Allow voice message access across the community boundaries
- Deny voice message access across the community boundaries

Authorization Codes

Authorization codes are associated with class of restriction (COR). If you want to assign a unique set of authorization codes to a tenant, you create a unique set of CORs. You only assign the CORs to objects that are within the partition that the tenant uses.

Automatic Wakeup

Those who control a tenant partition assign a music source to the partition. The system uses this music source as the wakeup music for users in the partition.

Bridged Call Appearance

Assign all stations with bridged call appearances to the same tenant.

Call Coverage

The tenant-to-tenant access restrictions apply to coverage paths. The system does not allow a call to cover to a tenant if the tenant-to-tenant access restrictions do not allow the user to call the tenant.

When you specify an attendant in a coverage path, the system accesses the attendant group of the called tenant. The system does not access the attendant group of the calling tenant.

When the system uses the Call Coverage feature for a call, and a user answers the call and then places the call on hold, the system plays the music-on-hold music that is assigned to the original called party.

Call Detail Recording (CDR)

CDR does not report the tenant partition number of the extension or the trunk group that the system uses. You must infer the tenant partition number from the extension or the trunk-group number.

Call Pickup

Assign all stations in a call-pickup group to the same tenant. The system supports Call Pickup only if the caller and the called party can both call the pickup user. The caller and the called party do not need to be in the same pickup group.

Call Vectoring and Vector Directory Number (VDN)

When the system routes a call to a new destination as a result of a vector step, the caller hears the music that is assigned to the last active VDN.

While a call is in vector processing, the system uses the tenant number that is assigned to the active VDN, as determined by VDN Override, to select the music source for callers on hold. Note the following exception. If you use a **wait-time <time> hearing** <*extension*>**then <treatment 2>** command, where the <*extension*> is a music source, that music source plays instead of the music source that is associated with the active VDN.

The COR that is assigned to the VDN must allow music-on-hold.

Call Management System (CMS)

You can administer CMS to provide CMS reports to each tenant. You can restrict each CMS login to control, on a permission basis, only those entities that are assigned to a particular tenant. Outputs to separate printers allow any tenant to print their own CMS reports. The tenant-partitioning provider must administer CMS to provide this separation of tenant permissions.

Call Coverage and Tenant Partitioning

If a covered call does not route to an attendant in the first tenant group, you can route it to an attendant group of a different tenant partition. For example, you can reroute a call to Tenant Group B if the call is to cover to an attendant for Tenant Partition A but does not route to the attendant or is received out of hours when Attendant Group A is unstaffed.

To reroute the covered calls to another tenant attendant group, Tenant Attendant group B in this example,

1. In the vector for the tenant A attendant vectoring VDN, add a failure branch to a **route-to ldn_number with cov y if unconditionally** step for the LDN extension for the tenant group B TN number.
2. Set the **with coverage** parameter of the route-to step must be set to **cov y** because the calls are covered. Else, the calls don’t route to the VDN. Also, set the **Cvg Enabled for VDN Route-to party?** field of original coverage path, which covers to Tenant A Attendant vectoring VDN, to **y**.

Dial Access to Attendant

When a tenant dials an attendant, the tenant accesses the attendant group to which the tenant is assigned.

Emergency Access to the Attendant

When a tenant dials the emergency access, the tenant accesses the attendant group to which the tenant is assigned.

Expert Agent Selection (EAS)

The COR that you assign to the logical agent ID in the EAS system determines whether callers that are on hold hear music. The COR that you assign to the physical extension does not control whether callers that are on hold hear music.

Hunt groups

The tenant number that you assign to the hunt group extension determines the music source that the callers to the hunt group hear while the callers are in queue or on hold.

Intercept Treatment

When access to the attendant is designated as intercept treatment, the caller accesses the attendant group to which the caller is assigned.

Malicious Call Trace (MCT)

The system assigns MCT extensions to tenant partition 1 as the default for the system. If MCT is enabled, any user who has permission to call tenant partition 1 can use MCT.

Multiple Listed Directory Numbers (LDNs)

Assign a tenant partition to each LDN.

Multiple Audio and Music Sources for Vector Delay

When you specify the audio source by a **wait-time <time> hearing <treatment>** vector step, the audio source that is assigned to the tenant number of the active VDN is the audio source that plays.

If you use a **wait-time <time> hearing** <*extension*>**then <treatment 2>** command where the <*extension*> is an audio source, that audio source plays instead of the audio source that is associated with the active VDN. For information on administering multiple audio sources, see the *Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780.

Music-on-Hold Access

You can assign a unique source for music to each tenant.

Night Service

Each tenant can have a listed directory number (LDN) night destination, a trunk answer on any any station (TAAS) port, or a night attendant that only the tenant uses.

PC Interfaces

You must assign each PC interface to a tenant partition.

PC/PBX Connections

You must assign each PC/PBX Connection to a tenant partition.

PC/ISDN

You must assign each PC/ISDN to a tenant partition.

Remote Access

You must assign each remote access barrier code to a tenant.

Traffic Studies

Traffic studies do not report the tenant partition number of the extension or the trunk group. You must infer the tenant partition number from the extension or trunk-group number.

Uniform Dial Plan (UDP)

If a UDP is in place between servers, the system does not pass tenant partition identification between the servers. The system does not enforce tenant-partition restrictions between the servers unless you provide special administration.

Tenant Partitioning restrictions do not override COR restrictions. COR restrictions are independent of tenant partitions.

Chapter 180: Terminal Translation Initialization

Use the Terminal Translation Initialization (TTI) feature to merge an X-ported extension to a valid port, or to separate an extension from a port.

Detailed description of Terminal Translation Initialization

Use TTI to:

- Merge an X-ported extension to a valid port. To merge an X-ported extension to a valid port, enter the system-wide TTI security code, and then the extension from a telephone that is connected to the valid port.
- Separate an extension from the port to which the extension is assigned. To separate the extension from the port, enter the required numbers. When you enter the required numbers, the extension is administered as an X port.

When TTI is enabled for voice, all voice ports, except Basic Rate Interface (BRI) ports, become TTI ports, or ports from which a TTI merge sequence can occur.

You usually use TTI to move telephones. However, you can also use TTI to connect and move attendants and data modules.

Note:

You cannot perform TTI merge on DCP deskphones after restarting Communication Manager. To resolve this issue, you must press any other call appearance and then perform TTI merge.

Using TTI with attendant consoles

About this task

You must assign an extension to the attendant console, if you want the attendant to use TTI.

TTI port translations are the same for both digital telephones and attendant consoles. To merge a digital TTI voice port and an attendant console, you must:

Procedure

1. Administer the attendant console as an X port.

2. Plug a digital telephone into the jack that is assigned to the attendant console.
3. Enter the TTI merge digit sequence at the digital telephone.
4. Unplug the digital telephone.
5. Plug the attendant console into the jack.

   You can separate an attendant console from its port only through administration. A TTI separate request from an attendant console gives the user intercept treatment.

   Note:

   If you want to use TTI, you must assign a call appearance (call-appr) to the first button position. TTI needs the button on the first call appearance to get dial tone.

Using TTI with data modules

About this task

The system provides status information during the TTI merge, and the separate operations on a telephone that is connected to a data module. If the **TTI State** field on the Feature-Related System Parameters screen is set to data, the system displays the status information. If the **TTI State** field on the **Feature-Related System Parameters** field is set to voice, the system generates tones to indicate status.

For a standalone data module, you enter the TTI merge and separate digit sequence on one line at a DIAL prompt:

Procedure

DIAL: **<TTI feature access code><TTI security code><extension>**

The system does not generate separate prompts for the TTI security code and the extension.

TTI with voice and data telephones

The system process a telephone with a data terminal (DTDM) as a telephone in the TTI merge and separation sequence operations. The DTDM is merged with and separated from its hardware translation at the same time that the telephone is merged or separated. You can start the TTI merge and separate sequence only through the telephone. You cannot start the sequences for DTDMs through the data port.

TTI with ISDN-BRI telephones

You use the same TTI separation sequence for Automatic-TEI SPID-initializing BRI telephones that you use for other telephones. However, the merge sequence is different.

Separating an ISDN-BRI telephone with TTI

Procedure

1. Feature access code (FAC)
2. Security code

3. Extension

Merging an ISDN-BRI telephone with TTI

Procedure

1. Connect the telephone to any port to get power.
2. Program the service profile identifier (SPID) to the extension with which the telephone is to be merged.
3. Unplug the telephone.

   You must unplug the telephone, even if the telephone is connected to the intended port.
4. Connect the telephone to the intended port.

   The intended port must indicate Equipment Type: TTI Port.
5. Listen for the dial tone.
   - If you hear dial tone, the merge is complete.
   - If you do not hear dial tone, the SPID of the telephone is an unavailable extension.

   You can dial the TTI merge sequence for BRI telephones only if a user separates a BRI extension from its telephone, and then wants to reassociate the telephone to the same extension. You cannot use the system access terminal (SAT) to put an x in the **Port** field of a BRI Station record that is still connected to the server that runs Communication Manager. You must use the TTI separation sequence from the telephone.

TTI for analog queue warning ports and external alert ports

You can administer the analog queue warning port that is used for hunt groups, and the external alert port, with an x in the **Port** field. You can use TTI to merge these extensions to an analog port. You must perform the merge at an analog set, and then unplug the analog set from the port. You cannot use TTI to separate these extensions from their port location. A TTI separate request from one of these ports gives you intercept treatment.

TTI security

Security alert:

If you do not manage TTI carefully, unauthorized use of this feature can cause you security problems. For example, someone who knows the TTI security code can disrupt normal business functions by separating telephones or data terminals. You can help protect against unauthorized use of TTI by frequently changing the TTI security code. To further enhance system security, remove the Feature Access Code (FAC) from the system when the FAC is not needed. Consult the Avaya Products Security Handbook for additional information to secure your system, and to find out about regularly obtaining updated security information.

Erase user data from DCP telephones

Beginning with Communication Manager Release 4.0, administrators can delete local information that is stored in a DCP telephone (2410 and 2420 sets only) when the telephone is reset by a PSA logoff or similar event. Depending on Communication Manager administration, this feature might eliminate the telephone's local speed dial lists, call logs, language, button labels or customized option settings that were defined by the user and may be of a personal nature.

System administrators are able to re-assign terminals without the need to send a technician to user's desk to manually erase the data.

Any of the following events can erase the following local data items from the 2420 and R2 of the 2410 DCP sets

- PSA disassociate & TTI unmerge
- A new **`erase terminal`** SAT command

Note:

Communication Manager does not erase data from an IP terminal upon receiving an unregistration request from the terminal. Using Avaya IP terminals, users cannot access local terminal information while the terminal is unregistered.

To administer this feature, use the following fields on the Class of Restriction screen:

- Use the **ERASE 24xx USER DATA UPON Dissociate or unmerge at this phone** field to administer what local terminal data items are erased when the 24xx is dissociated or unmerged.

For more information on the values and defaults for these fields, see *Avaya Aura® Communication Manager Screen Reference*.

For more information on the new **`erase terminal`** SAT command, see *Maintenance Commands for Avaya Aura® Communication Manager Branch Gateways and Servers*.

Terminal Translation Initialization administration

This section describes the screens that you use to administer the Terminal Translation Initialization feature.

Screens for administering Terminal Translation Initialization

Screen name	Purpose	Fields
Attendant Console	Define an attendant console.	All
Data Module	Define a data module.	All

Table continues…

Screen name	Purpose	Fields
Feature Access Codes (FACs)	Create FACs for the TTI merge and separate operations.	• Terminal Translation Initialization Merge Code • Terminal Translation Initialization Separation Code
Feature-Related System Parameters	Enable TTI for the system.	• TTI Enabled • TTI State • TTI Security Code
Station	Define a station.	All

Interactions for Terminal Translation Initialization

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

Attendant

You can separate an attendant if the attendant is in Position Available Mode. However, you cannot separate an attendant if any calls are in the queue, held, or active for the attendant.

Attendant Night Service

You cannot separate the night service station, when the station is in night service.

Attendant Release Loop Operation

If the attendant separates before the attendant-timed reminder-interval expires, the system reclassifies all calls that are held with the release loop operation by the attendant as attendant group calls.

Automatic Callback

If you use TTI to separate either telephone that is part of Automatic Callback, the system breaks the automatic callback sequence.

Call Coverage

Send All Calls and Go to Coverage remain active, while the telephone has no associated hardware.

You can separate a telephone that is the receiver of Send All Calls or Go to Coverage. The system processes calls to the telephone as if the telephone is busy.

Call Coverage Answer Group

If an extension that was an X port rejoins a call coverage answer group as a result of a TTI merge, the system excludes the extension from all transactions that are already active in the call coverage answer group.

Call Forwarding

You can separate a telephone while Call Forwarding is active. If a destination extension for call forwarding separates, Call Forwarding to that extension remains active. The system processes calls to the telephone as if the telephone is busy.

Call Pickup

If a line appearance is available, a member of a call pickup group can separate at any time. If a call is attempting to terminate, and a member of a group associates, that member does not join the group for the call that is currently in progress. The member can participate in all subsequent calls to the call pickup group.

Expert Agent Selection (EAS)

Station user records cannot be shared between TTI ports and Expert Agent Selection (EAS) login ID extensions. For example, if you administer 2,000 EAS login IDs, the maximum number of TTI ports that the system can provide is reduced by 2,000.

Hunt Group Uniform Call Distribution (UCD) and Direct Department Calling (DDC)

The system excludes telephones that are previously X-ported as a result of a TTI separation request from all transactions that are already active in the hunt group when the telephone is merged.

Site Data

If TTI is enabled, the system displays a warning message after you administer the Site Data fields.

If TTI is enabled, and you change the **Port** field on the Station screen from x to a port number, and change the **Room**, **Jack**, or **Cable** fields in the **Site Data** section of the Station screen, the system displays a warning message when you tab off the fields.

Terminating Extension Group (TEG)

If any member of a TEG that was previously an X port as a result of TTI is merged, the member is excluded from all transactions that are already active in the TEG when the member is merged. The member can join all subsequent calls to the group.

Chapter 181: Terminating Extension Group

Using the Terminating Extension Group (TEG) feature, an incoming call can ring as many as four telephones at one time. Any user in the group can answer the call.

Detailed description of Terminating Extension Group

You can administer any telephone as a TEG member. However, only a multiappearance telephone can be assigned a **TEG** button with a merged-status lamp. With the **TEG** button, the user can select a TEG call appearance to answer or bridge onto an existing call, but not to originate the call. The TEG members are assigned on an extension number basis. Call reception restrictions applicable to the group are specified by the class of restriction (COR) for the group. The group COR takes precedence over an individual member’s COR. When a Terminating Extension Group (TEG) receives an incoming call, the TEG's primary Class of Restrictions (COR) is considered for the calling and called restrictions. The members could all be termination-restricted but still receive calls if the group is unrestricted.

When a TEG members answers an incoming call, a temporary bridged appearance is maintained at the multiappearance telephones in the group. However, this appearance is not visible. Any TEG member can press the TEG button to bridge onto the call.

Terminating Extension Group administration

This section describes the screens that you use to administer the Terminating Extension Group (TEG) feature

Screens for administering Terminating Extension Group

Screen name	Purpose	Fields
Terminating Extension Group	Define the groups for the TEG feature.	• Coverage Path • Group Name • Group Extension • COR • TN • ISDN Call Display • Ext

Considerations for Terminating Extension Group

This section provides information about how the Terminating Extension Group (TEG) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Terminating Extension Group under all conditions. The following considerations apply to Terminating Extension Group:

- A telephone user can be a member of more than one TEG, but can have only one **TEG** button for each group.
- A TEG can handle only one TEG call at a time. Additional calls do not reach the TEG. If a coverage path is assigned to the TEG, the system routes the additional calls accordingly.

Interactions for Terminating Extension Group

This section provides information about how the Terminating Extension Group (TEG) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Terminating Extension Group in any feature configuration.

Automatic Callback

This feature cannot be active for a TEG.

Bridged Call Appearance

Calls to a TEG cannot be bridged, except by way of a Temporary Bridged Appearance.

Call Coverage

A TEG can have a Call Coverage path assigned, but cannot be a point in a Call Coverage path.

A **Send Term** button for the TEG can be assigned to group members who have multiappearance telephones. When a user presses **Send Term**, the system redirects calls to the TEG redirect to

coverage. The merged status lamp lights on all telephones with a **Send Term** button. Any member with a **Send Term** button can press the button to deactivate **Send Term**. Incoming calls are directed to the group.

Call Park

A TEG call cannot be parked on the group extension. However, group members who answer a call can park a TEG call on their own extensions.

Direct Department Calling (DDC) and Uniform Call Distribution (UCD)

A TEG cannot be a member of a DDC or a UCD group.

Internal Automatic Answer

TEG calls are ineligible for Internal Automatic Answer. However, calls that are placed to an individual extension are eligible.

Leave Word Calling (LWC)

Leave Word Calling messages can be stored for a TEG. Any member of the group, covering user of the group, or system-wide message retriever can retrieve the stored messages. Telephone Display and proper authorization can be assigned to the message retriever. Also, a remote Automatic Message Waiting lamp can be assigned to a group member to provide a visual indication that a message has been stored for the group. One indicator is allowed per TEG.

Privacy - Manual Exclusion

Privacy - Manual Exclusion can be assigned to any of the telephones in a TEG to prohibit bridging by other group members. A TEG member who attempts to bridge onto a call with Privacy - Manual Exclusion active is dropped.

Temporary Bridged Appearance

At multiappearance telephones in the TEG, a temporary bridged appearance is maintained after a call is answered. Thus, other members of the group can bridge onto the call.

Chapter 182: Transfer

Using the Transfer feature, telephone users can transfer trunk calls or internal calls to other telephones or trunks without attendant assistance.

Detailed description of Transfer

Transfer supports the following capabilities:

- Pull Transfer
- Abort Transfer
- Transfer Recall
- Transfer Upon Hangup
- Trunk-to-Trunk Transfer
- Outgoing Trunk to Outgoing Trunk Transfer
- Emergency Transfer
- Name Display on Unsupervised Transfer

Pull Transfer

With Pull Transfer, either the transferring party or the transferred-to party can press the **Transfer** button to complete the transfer operation.

When attendants control calls, called parties cannot use Pull Transfer. Attendants who are called parties cannot use Pull Transfer. When attendants have parties on hold, the parties are transferred with the standard transfer process.

To use Pull Transfer, calling parties and called parties must be on the same server, or called parties must be reached by way of Italian TGU/TGE tie trunks.

Called parties who use analog telephones flash the switch hook, or press the flash key or recall button to transfer calls. Called parties who use digital telephones press the transfer key to complete transfers.

Abort Transfer

Use Abort Transfer to stop the transfer operation whenever a user presses a non-idle call appearance button in the middle of the transfer operation, or when the user hangs up. If both

the **Abort Transfer** and **Transfer Upon Hang-Up** fields are set to y and you press the **transfer** button, and then dial the complete transfer-to number, hanging up the telephone transfers the call. You must select another non-idle call appearance to abort the transfer. If the **Transfer Upon Hang-Up** field is y, hanging up completes the transfer. Requires DCP, Hybrid, IP, ISDN-BRI or wireless telephones

Transfer Recall

Use Transfer Recall to return the unanswered transfer call back to the person who transferred the call. Transfer Recall uses a priority alerting signal. The display on the telephone also shows “rt,” which indicates a returned call from a failed transfer operation.

Transfer Upon Hangup

Use Transfer Upon Hangup to disconnect the transfer of call without the need of pressing the **Transfer** button twice. You press the **Transfer** button, dial the number to which the call is being transferred, and then disconnect the call. Transfer Upon Hangup is an optional capability at the system level. You can still press the transfer button a second time to transfer the call.

Trunk-to-Trunk Transfer

With Trunk-to-Trunk Transfer, an attendant or a user can connect an incoming trunk call to an outgoing trunk.

Security alert:

Trunk-to-Trunk Transfer poses a significant security risk. Use this capability with caution.

The system provides three levels of administration for this Trunk-to-Trunk Transfer:

- Systemwide
- COR to COR
- COS

To administer Trunk-to-Trunk Transfer systemwide, complete the Feature-Related System Parameters screen. To restrict Trunk-to-Trunk Transfer on a trunk-group basis, assign COR-to-COR calling-party restrictions on the Class of Restriction screen. To allow individual users to control Trunk-to-Trunk Transfers, assign capabilities on the Class of Service screen.

Outgoing Trunk to Outgoing Trunk Transfer

With Outgoing Trunk to Outgoing Trunk Transfer (OTTOTT), a controlling party such as a station user or an attendant, initiates two or more outgoing trunk calls, and then connects the trunks. This operation removes the controlling party from the connection and conferences the outgoing trunks. The controlling party can also establish a conference call with the outgoing trunks, drop out of the conference, and leave only the outgoing trunks on the conference.

Note:

This capability is an optional enhancement to Trunk-to-Trunk Transfer and requires careful administration and use. The Distributed Communications System (DCS) Trunk Turnaround may be an acceptable and safer alternative to this feature.

With OTTOTT, you can establish calls in which the only parties involved are external to Communication Manager and are on outgoing trunks. This type of call can result in locked-up trunks, such as trunks that cannot be disconnected except by busying-out and releasing the affected trunk circuit. To clear the lockup, a service technician must reset the trunk board, or busy-out and release the affected trunk.

Name Display on Unsupervised Transfer

Communication Manager Release 4.0 or later displays transferred-to names on calls redirected with Call Transfer, to interoperate with the Tenovis I55. This enables sending the transferred-to station name (not answered enquire call) using the primary Private Integrated Network Exchange (PINX) after call transfer. The calling station screen displays the transferred-to name after receiving the name in the primary PINX.

Previously, when transferring to a not answered connection (primary connection was established through QSIG) the redirection name was not sent in the FACILITY message independent from the value of the **Send Name** field on the trunk group associated with the primary PINX QSIG trunk. Therefore the name of the transferred-to station (enquiry call) did not appear immediately after call transfer on the display of the station in the primary connection.

Now, When Station A calls B, and is transferred to C, Station B has established a connection through QSIG to station A and an enquire connection (internal or through QSIG) to station C. Station B transfers station C to station A. The name of Station C (not answered enquire call) is sent after call transfer to station A (through QSIG to primary PINX) when the **Send Name** field on the Trunk Group screen is set to y at the QSIG trunk side to the primary PINX. So the name of the transferred-to station C appears on the display of the station A in the primary connection immediately after the call transfer.

To administer this capability, you must set the **QSIG value-added** field to y on the Trunk Group screen. This matches the name and number on the extension. In addition, on the Trunk Group screen, there is a new function for the **Send Name** field. The existing values y(es), r(estrict), and n(o) values now also control the sending of the name at the QSIG trunk side.

y = send redirection Name

r, n = do not send redirection Name

For more information on these fields, see *Avaya Aura® Communication Manager Screen Reference*.

Transfer administration

This section describes the screens that you use to administer the Transfer feature.

Screens for administering Transfer

Screen name	Purpose	Fields
Class of Restriction	Define transfer options.	Block Transfer Display Block Enhanced Conference/Transfer Displays
Extensions To Call Which Activate Features by Name	Define transfer options.	Transfer Complete Transfer On Hang-Up Transfer to Voice Mail
Feature Access Code (FAC)	Define transfer options.	Transfer to Voice Mail Access Code
Feature-related System Parameters	Define transfer options.	Trunk-to-Trunk Transfer Music (or Silence) on Transferred Trunk Calls Internal Auto-Answer of Attd-Extended/ Transferred Calls Station Call Transfer Recall Timer (seconds) Abort Transfer Transfer Upon Hang-Up Pull Transfer Update Transferred Ring Pattern Copy ASAI UUI During Conference/ Transfer Intercept Treatment On Failed Trunk Transfers Pickup On Transfer SIP Endpoint Managed Transfer
Signaling group	Define transfer options.	Network Call Transfer
System Parameters Call Coverage/Call Forwarding	Define transfer options.	External Coverage Treatment for Transferred Incoming Trunk Calls
Trunk group	Define transfer options.	Send Transferring Party Information

Considerations for Transfer

This section provides information about how the Transfer feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Transfer under all conditions. The following considerations apply to Transfer:

- You can administer transferred trunk calls to receive either music or silence if the first part of the transfer places the call on hold.
- Multiappearance telephones must have an idle appearance to transfer a call.
- Single-line telephone users momentarily flash the switch hook or press the **Recall** button, dial the required extension, and disconnect. Multiappearance telephone users press the **Transfer** button, dial the required extension, and press the Transfer button again.
- If, on the Feature-Related System Parameters screen, the **Transfer Upon Hang-up** field is set to y, users can transfer a call by pressing the **Transfer** button, dial the required extension, and then disconnect. Users can disconnect while the required extension is ringing or after the party has picked up. The user also can still press the **Transfer** button a second time to complete the transfer process.
- If, on the Feature-Related System Parameters screen, the **Abort Transfer** field is set to y, users press the **Transfer** button, dial the required extension, and then disconnect or select any non-idle call appearance. The user must press the **Transfer** button again to complete the process (see Note). If the user selects an idle call appearance, the transfer is still active.

  Note:

  If both, the **Abort Transfer** and the **Transfer Upon Hang-Up** fields, are y and you press the **Transfer** button and then dial the complete transfer-to number, hanging up the telephone transfers the call.
- Users of Digital Communications Protocol (DCP), hybrid, and wireless telephones can transfer a call that is on hold without removing the call from hold. If only one call is on hold, no active call appearances exist, and call appearance is available for the transfer, the user can transfer the call simply by pressing the **Transfer** button. Communication Manager assumes that the transfer is for the call on hold, and the transfer feature works as usual.

  If more than one call is on hold, the user must make a call active to transfer it. If the user presses the **Transfer** button with two or more calls on hold, Communication Manager ignores the transfer attempt since it will not know which call the user wants to transfer. If there are calls on hold and an active call, pressing the **Transfer** button will start the transfer process for the active call.
- Communication Manager can be administered to display a confirmation message to users upon successful call transfers. The confirmation message is visible to users with DCP, Hybrid, wireless (except for 9601), or Integrated Services Digital Network-Basic Rate Interface (ISDN-BRI) display telephones. These telephones, except for the hybrids, can display the confirmation message in English, Spanish, French, Italian, or a language that you define. Hybrid telephones can display the message in English only.
- You can administer the system to return a transferred call to the originator if the transferred-to party does not answer within a set time limit. To do this, enter a value in the **Station Call**

Transfer Recall Timer field on the Feature-Related System Parameters screen. For any transfer if **SIP Endpoint Managed Transfer** feature is applied then the station recall will not start. For information on how to administer the **SIP Endpoint Managed Transfer** feature, see *Administering Avaya Aura® Communication Manager*.

The following consideration is for Outgoing Trunk to Outgoing Trunk Transfer (OTTOTT):

- OTTOTT is not intended for use in DCS networks, since DCS Trunk Turnaround provides comparable capabilities much more safely. However, use of OTTOTT with DCS is not prohibited, and might be useful when one or more of the trunks goes off the DCS network.

The following considerations are for Trunk to Trunk Transfer:

- Trunk-to-Trunk Transfer is particularly useful when a caller outside the system calls a user or attendant and requests a transfer to another outside number. For example, a worker, away on business, can call in and have the call transferred elsewhere.
- Transferred trunk calls can be administered to receive either music or silence.
- Some CO trunks do not signal the PBX when the CO user disconnects from a call. The system ensures that incoming CO trunks without Disconnect Supervision are not transferred to outgoing trunks or to other incoming CO trunks without Disconnect Supervision.
- An attendant-assisted call connecting an outgoing trunk or incoming trunk without Disconnect Supervision to an outgoing trunk must be held on the console. The attendant cannot release the call. The attendant can, however, use the Forced Release button and disconnect all parties associated with the call.
- If a user has connected two outgoing trunks or an outgoing call and an incoming call without Disconnect Supervision, the user must remain on the call. Otherwise, the call is dropped. An incoming trunk with Disconnect Supervision can be connected to an outgoing trunk without the user remaining on the call. An incoming trunk can also be connected to another incoming trunk without the user remaining on the call if one of the incoming trunks has Disconnect Supervision.

Interactions for Transfer

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

Analog Station Recall Operation and Feature Activation

When called parties initiate either analog-telephone recall or feature activation, callers are not put on hold for transfer. Instead, callers are transferred by way of Pull Transfer.

Basic Rate Interface (BRI) telephones

Callers who use BRI Stations reach required parties through the intermediate step of calling a party who calls a final destination. Intermediate parties activate pull transfer to complete transfers. Final called parties go off hook as if a new transfer were originated.

Call Detail Recording (CDR)

The software checks to ensure that calls are correctly recorded with CDR when Pull Transfer is completed.

Digital Station Transfer Operation

When called parties initiate transfer operations, callers are not put on hold for transfer; they are transferred by way of Pull Transfer.

Non-BRI telephones

Callers who use the non-BRI telephones reach required parties through an intermediate step of calling a party who calls a final destination. Each called party activates pull transfer.

The following interactions are for Outgoing Trunk to Outgoing Trunk Transfer (OTTOTT):

DCS Trunk Turnaround

OTTOTT increases the set of cases in which DCS Trunk Turnaround can be accepted. However, use of OTTOTT in combination with a DCS network is strongly discouraged. The following algorithm describes the DCS Trunk Turnaround request process.

- If any party on the call receives a local-dial, busy, intercept, or reorder tone, deny turnaround. If any remaining party is an answered station or attendant, accept turnaround.
- If any remaining party is on an incoming trunk, accept turnaround. For the purposes of this check, an outgoing DCS trunk that has been turned around an odd number of times by way of a DCS trunk turnaround is considered an incoming trunk with disconnect supervision. Similarly, an incoming DCS trunk that has been turned around an odd number of times is considered an outgoing trunk.
- If any remaining party is an outgoing trunk administered for OTTOTT that has received answer supervision, accept turnaround.
- If any remaining party is an outgoing DCS trunk, forward the turnaround request.
- If any remaining party is not a DCS trunk, deny turnaround.

Incoming Disconnect Supervision

Outside of the US, incoming disconnect supervision is a switching capability that restricts transfers or conferences for certain incoming trunks. In the U.S., all incoming trunks are assumed to provide disconnect supervision. In some countries, this assumption is invalid. Therefore, you must administer whether or not an incoming trunk provides disconnect supervision for each trunk group.

Personal Central Office Lines (PCOLs)

Transfer of PCOLs is not subject to the normal restrictions that are applied to transfer of other trunks. These transfers are allowed since the PCOL appearance remains on one or more stations as a feature button. System users must be aware that the DROP button cannot be used to disconnect the transferred-to party from the call. Therefore, if an outgoing PCOL is transferred to an outgoing trunk and neither of the trunks can supply a disconnect signal, the two trunks lock up.

Pull Transfer

If station A is talking to station B and station B begins a transfer to station C, only station C can use the Pull Transfer feature to grab the call. Furthermore, if station B uses the Toggle Swap feature to return to station A and station C is now in a soft hold state, station C cannot use the Pull Transfer feature until station B toggles back and has station C in the talk state.

QSIG Global Networking

If either call is over an ISDN-PRI trunk that is administered with Supplementary Service Protocol b (QSIG), the system might display additional call information.

Release-Link Trunks (RLT)

RLTs are used by CAS. An outgoing RLT at a remote branch is used to access an attendant at the main. The attendant at the main can transfer the incoming caller to a station or a trunk at the branch. The RLT is typically used only for a short period of time and is usually idled after the transfer is established.

A station at a branch can transfer an outgoing trunk to the attendant at the main. This transfer could be viewed as an OTTOTT (the attendant is accessed by way of an outgoing RLT). Since administering outgoing disconnect supervision for RLT trunks provides no additional capability, this administration is not provided for RLT trunks.

Restriction

Restrictions on the transferring party can block a transfer or a drop operation even when Outgoing Disconnect Supervision is provided.

Trunk-to-Trunk Transfer

If this feature-related system parameter is set to Restricted, all trunk-to-trunk transfer or release, or drop operations for public trunks (CO, CPE, CAS, DID, DIOD, FX, and WATS) have calls terminated or receive denial. If the parameter is set to None, all trunk-to-trunk transfers (except CAS and DCS) have calls terminated or receive denial.

Hence, you use All to enable OTTOTT operation for these types of trunks. The number of public network trunks allowed on a conference call is administrable. This number defaults to 1, so if OTTOTT is being used to connect two or more public network trunks, you must increase this limit on the Feature-Related System Parameters screen.

Trunks (CO, FX, and WATS)

You cannot have two CO, FX, or WATS trunks in a OTTOTT connection, even if the **Disconnect Supervision - Out** field is set to y.

The following interactions are for Trunk to Trunk Transfer:

Attendant Lockout

Attendant Lockout does not function on Trunk-to-Trunk Transfer.

Call Vectoring

Station control of Trunk-to-Trunk Transfer does not affect routing of incoming trunks to a vector directory number (VDN) that ultimately routes to a destination off-net.

A route to a number off-switch does not require you to enable trunk-to-trunk transfer.

Tenant Partitioning

Station control of Trunk-to-Trunk Transfer is prohibited between trunks in different tenant partitions if those partitions are restricted.

The following interaction is for Emergency Transfer:

Night Service

If a power failure occurs when the system is in night service, the system automatically returns to night service when power is restored.

Chapter 183: Trunk Flash

Using the Trunk Flash feature, user of a multifunction telephone or an attendant console can access far-end customized services or central office (CO) customized services.

Detailed description of Trunk Flash

With Trunk Flash, a user of a multifunction telephone or an attendant console can gain access to far-end customized services or central office (CO) customized services. To use Flash Trunk, the user presses the flash button or dials the Feature Access Code (FAC) for Trunk Flash.

CO customized services are electronic features, such as conference and transfer, that are accessed by a sequence of flash signal and dial signals from a Communication Manager telephone on an active trunk call. The Trunk Flash feature can help to reduce the number of trunk lines that are connected to the server that runs Communication Manager by performing:

- Trunk-to-trunk call transfers at the far-end or the CO, which eliminates the use of a second trunk line for the duration of the call, and frees the original trunk line for the duration of the call.
- A conference call with a second outside call party, which eliminates the need for a second trunk line for the duration of the call.

Note:

Some analog dual-tone multifrequency (DTMF) telephone sets that are used in Italy and the United Kingdom have a **Flash** button. When a user presses that **Flash** button, the button generates a rotary digit 1. When an analog telephone that is administered as a DTMF telephone, for example, as a 2500 or a 71nn-type telephone, transmits a rotary digit 1, the system processes the signal as a recall signal from the telephone set to Communication Manager.

A centralized attendant service (CAS) attendant who is connected to a release line trunk (RLT), the **Flash** button controls certain CAS features at the branch. For a user of a multifunction telephone or non-CAS attendant connected to a CO, foreign exchange (FX), or a Wide Area Communications Service (WATS) trunk, the flash controls certain features, such as add-on, at the connected CO.

Trunk Flash is unavailable on Personal Central Office Line (PCOL) groups.

The system supports the Trunk Flash signal for incoming, outgoing, or two-way call directions on selected two-wire analog or digital DS1 trunks, or tie trunks on DS1.

If the trunk group is a DS1 trunk in Italy, the Trunk Flash feature applies only to outgoing calls.

If the trunk is indirectly connected to the far-end or the CO that provides the customized services, use of the Trunk Flash signal can cause the far end or the CO to disconnect the call.

The system does not record Call Detail Recording (CDR) information for calls that a user makes with the Trunk Flash feature.

Trunk Flash administration

This section describes the screens that you use to administer the Trunk Flash feature.

Screens for administering Trunk Flash

Screen name	Purpose	Fields
Feature Access Code (FAC)	Assign a FAC for Trunk Flash.	Flash Access Code
Trunk Group	Enable Trunk Flash for the trunk group.	Trunk Flash

End-user procedures for Trunk Flash

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

Using Trunk Flash

Procedure

1. Press the **Flash** button.
2. Dial the FAC for Trunk flash.

Considerations for Trunk Flash

This section provides information about how the Trunk Flash feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Trunk Flash under all conditions. The following considerations apply to Trunk Flash:

Caution:

Using the Trunk Flash feature, the telephone user can receive central office (CO) dial tone. A user can place a call that is not monitored by Communication Manager, and is not subject to restrictions such as toll, facilities restriction level (FRL), and class of restriction (COR). Use caution when you enable this feature.

- A Trunk Flash button can be assigned on CAS attendant consoles, non-CAS attendant consoles, and multifunction telephones. For CAS attendants, use of this button is limited to certain CAS features by way of RLT trunks. For multifunction and non-CAS attendant consoles, this button is used for the Trunk Flash feature.
- FAC activation of the trunk flash feature is allowed.
- System features, such as internal conference call, transfer, and call par, can be combined with custom services. The custom services are CO-based features that are activated/controlled by sending a flash signal over the trunk to the CO. However, mixing Communication Manager features with custom services causes complications for the user when the user tracks a call. Communication Manager cannot give the local telephone user status information on the custom services.
- The Trunk Flash feature can only be accessed if the call has only one trunk. The trunk must be an outgoing trunk and the **Trunk Flash** field on the Trunk Group screen must be set to y. The Trunk Flash feature is disabled when the call involves more than one trunk, even if all the trunks have Trunk Flash enabled.
- The system supports five users to participate in a conference call with the trunk line party. However, to access the Trunk Flash feature, at least one of the user telephones must have a **Flash** button.
- With a call that involves more that one user, one of the users can press the **Flash** button, and another user can dial the telephone number. The user that dials the telephone number is not required to have a telephone with a **Flash** button.

  If the far-end or the central office (CO) does not support custom services, the far-end or the CO can ignore the call or drop the call. If the far-end or the CO ignores or drops the call, the user might hear a clicking sound or the user might hear silence.

Chapter 184: Uniform Dial Plan

Use the Uniform Dial Plan (UDP) feature to share a common dial plan among a group of servers. The UDP applies both interserver dialing and intraserver dialing. The UDP provides the dial plans from 3 to 18 digits.

UDP provides extension-to-extension dialing between two or more private-switching systems.

You can use UDP with the following entities:

- Main servers
- Tributary servers
- Satellite servers
- Electronic Tandem Networks (ETN)
- Distributed Communication Systems (DCS)

Note:

You must use a 4-digit dial plan or a 5-digit dial plan for DCS.

Detailed description of Uniform Dial Plan

The software uses the UDP to route a call off the local server. The user dials an extension that consists of 3 to 18 digits. The software converts the extension that the user dials into a private-network number or a public network number.

To convert the extension, the software substitutes digits at the front of the extension that the user dials. The software supports the following types of extension conversions:

- Automatic Alternate Routing (AAR)

  The system uses AAR routing information to route calls within your company over your own private network.

  The software converts the number that the user dials. The software then analyzes the number, and routes the call as a private-network call.
- Automatic Route Selection (ARS)

  The system uses ARS routing information to route calls that go outside your company over public networks. The system also uses ARS routing information to route calls to remote company locations if you do not have a private network.

The software converts the number that the user dials. The software then analyzes the number, and routes the call as a public network call.

- Extension number portability (ENP)

  If you want calls on your system to use ENP conversion, you must specify a node number. The software uses the node number to determine the routing pattern for the call. If the user dials an extension that consists of 4 to 6 digits, the software chooses an ENP code that is based on the first 1 or 2 digits of the extension. The software does not use the ENP code for routing. Therefore the ENP code is independent of location.

- Extension (EXT)

  The system uses EXT conversion to analyze the extension that the user dials.

  Unlike AAR conversion or ARS conversion, the system might not change the extension that the user dials, before the system routes the call. If no UDP entry for a particular extension or for a range of extensions exists, the system considers the extensions to be local extensions.

You specify a UDP for individual extensions or groups of extensions that have the same leading digits. For example, if you use a 5-digit UDP, and choose a matching pattern of “123”, all 5-digit extensions that begin with “123” have the same UDP conversion scheme. If you use a 5-digit UDP, and want the software to use the UDP for only one extension, you must create a matching pattern that is the same as the extension. For example, if you choose a 5-digit UDP for extension 12345, you must specify 12345 as the matching pattern.

Each user extension can be assigned to one of the following six treatments:

- UDP Code
  - Conversion to AAR with a given location code
  - Further conversion is suppressed
- AAR Code
  - Conversion to AAR with a given location code
  - Further conversion is suppressed
- ENP Code
  - Conversion to a private-network number
  - Route to the given node number routing
- Temp OOS
  - Temporarily out of service
  - Give reorder
- Local

  Local range of extensions
- Blank

  This treatment is similar to local, but the system bypasses the when you perform an **`add station`** command.

When a user dials an extension that is on a server that is included in a UDP, the software firsts determines if the extension is assigned to a local station on the server. If the extension is assigned to a local station on the server, the software routes the call to the station. The software does not convert the extension numbers.

When a user dials an extension that is not on the server, the software compares the extension with the matching patterns. If the software finds a match between the extension and the matching patterns, the software converts the extension into a private network number. The software then routes the call as specified by the conversion.

When a user dials an extension, and the extension matches more than one matching pattern, the software selects the pattern that has the most matching digits. The software compares the extension and the matching pattern starting with the first digits that the user dials through to the last digits. See the table on page 1380, for examples of matching patterns.

If the extension does not match a matching pattern, and Extended Trunk Access (ETA) is enabled on the system, the software uses ETA to route the call. If the extension does not match a matching pattern, and ETA is disabled on the system, the user receives intercept treatment.

Table 122: Matching pattern selections

Extension dialed	Matching patterns available	Matching pattern selected
123	123 and 1234	123
12345	123 and 1234	1234
12355	123 and 1234	123

Uniform Dial Plan example

The section contains an example of UDP administration, and the processing of several calls that use UDP.

To administer UDP, you must assign each UDP code:

- To a private network location code (RNX) or node number. The RNX is equivalent to the office code of a central office (CO) in a public network. This RNX determines how the system routes a UDP call.
- As either local or remote to Communication Manager.

The same 5-digit extension is used to call a station, regardless of where in the electron tandem network (ETN) that call originates. This example includes three media servers or switches (the table on page 1380). Each media server and switch has a list of RNX and UDP codes.

Table 123: RNX and UDP codes

Media server or switch	RNX code	UDP code
A	224	41
C	223	51

Table continues…

C	223	52
B	222	60
B	222	61

See the figure on page 1381 for an example of a UDP scenario.

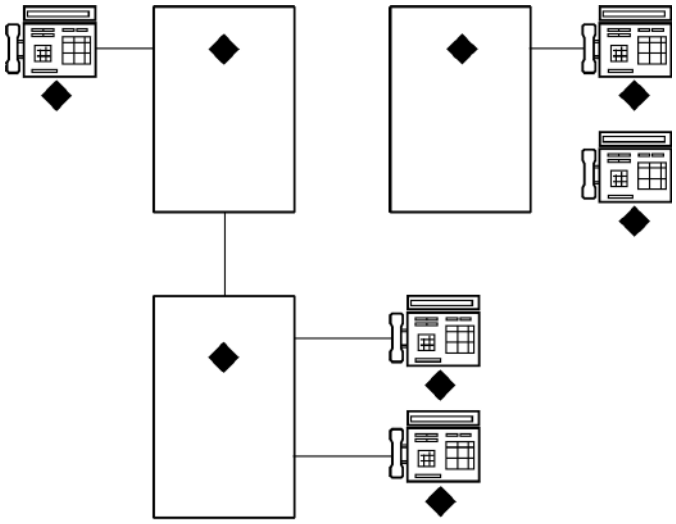


Figure 33: UDP Example

Table 124: Figure notes:

1. System A. The dial plan for the extensions is 41. The RNX is 224. 2. System B. The dial plan for the extensions is 60 and 61. The RNX is 222. 3. System C. The dial plan for the extensions is 51 and 52. The RNX is 223.	1. Extension 41000 2. Extension 61234 3. Extension 60123 4. Extension 51234 5. Extension 5200

A user at extension 41000 who wants to call extension 61234, has one of the following options:

- Dial 61234
- Dial the AAR access code, and then dial 222-1234

If the user dials 61234, the system:

- Recognizes 61 as a remote UDP
- Determines that the associated RNX is 222
- Uses AAR to route the call to 222-1234

If the user dials the AAR access code and 222-1234, the system:

- Finds the route pattern for RNX 222
- Routes the call to the server that is associated with that RNX

When the software uses UDP to route a call to another server or system, the route pattern provides the correct digit deletion and insertion instructions. The receiving system then gets numbers in the format that the receiving system expects.

You can configure the software several different ways.

- If AAR is available on the receiving media server or switch:
  - Subnetwork trunking can be used to insert the Feature Access Code (FAC) for AAR on the server or switch where the call originates
  - Digit insertion can be used to insert the FAC for AAR on the receiving server

    The receiving server uses AAR digit conversion to delete 3 digits and add the digit 6, thus converting the number 222 with 7 digits to an extension.
- If AAR is unavailable on the receiving media server or switch, subnetwork trunking must be used on the originating server or switch to delete the 222 and insert the digit 6 at the start of the extension number. This conversion ensures that the receiving server can continue to route the call correctly.

If the user at extension 51234 on media server C dials extension 61234, the call must first go through media server A before the call goes to media server B. When the user dials 61234:

- The software recognizes 61 as a UDP code.
- The software determines that the associated RNX is 222, and uses the AAR feature to route the call.
- The FAC for AAR plus the digits 222-1234 are outpulsed to media server A.
- Media server A then recognizes the RNX 222 as a remote server or switch, and routes the call to media server B and extension 61234.

This same type of call routing occurs when an extension at media server B calls an extension at media server C.

If extension 61234 on media server B calls extension 60123, the software recognizes 60 as a local UDP code, and the system routes the call directly to extension 60123.

Uniform Dial Plan administration

The following tasks are part of the administration process for the Uniform Dial Plan (UDP) capability:

- Creating AAR and ARS Feature Access Codes for UDP
- Administering the Uniform Dial Plan table
- Administering the Node Number Routing Table for UDP
- Administering the AAR Digit Conversion Table for UDP

- Administering the ARS Digit Conversion Table for UDP
- Administering the AAR Digit Analysis Table for UDP
- Administering the ARS Digit Analysis Table for UDP
- Administering the extension number portability numbering plan

Related links

[Creating AAR and ARS Feature Access Codes for UDP](#) on page 1384
[Administering the Uniform Dial Plan table](#) on page 1384
[Administering the Node Number Routing Table for UDP](#) on page 1385
[Administering the AAR Digit Conversion Table for UDP](#) on page 1385
[Administering the ARS Digit Conversion Table for UDP](#) on page 1386
[Administering the AAR Digit Analysis Table for UDP](#) on page 1387
[Administering the ARS Digit Analysis Table for UDP](#) on page 1389
[Administering the extension number portability numbering plan](#) on page 1392

Preparing to administer Uniform Dial Plan

Procedure

On the Optional Features screen, ensure that the **Uniform Dialing Plan** field is set to y. If the **Uniform Dialing Plan** field is set to n, your system does not support the Uniform Dial Plan feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Uniform Dial Plan, or to open a service request.

To view the Optional Features screen, enter `display system-parameters customer-options`.

Screens for administering Uniform Dial Plan

Screen name	Purpose	Fields
Uniform Dial Plan Table	Define the type of conversion, the matching pattern, and the insertion digits.	All
AAR Digit Analysis Table	Define Automatic Alternate Routing (AAR) digit analysis.	All
ARS Digit Analysis Table	Define automatic route selection (ARS) digit analysis.	All
AAR Digit Conversion Table	Define AAR digit conversion.	All
ARS Digit Conversion Table	Define ARS digit conversion.	All
Extension Number Portability (ENP) Numbering Plan	Define ENP codes.	All
Number Node Routing	Associate a route pattern with each node in the ENP subnetwork.	Route Pat

Table continues…

Screen name	Purpose	Fields
Route Pattern	Define the route pattern.	All
Optional Features	Ensure that the Uniform Dial Plan feature is enabled on your system.	Uniform Dialing Plan

Creating AAR and ARS Feature Access Codes for UDP

Procedure

1. Enter `change feature-access-codes`.
2. In the **Auto Alternate Routing (AAR) Access Code** field and the **Auto Route Selection (ARS)** field, perform one of the following actions:
   - If the **Auto Alternate Routing (AAR) Access Code** field and the **Auto Route Selection (ARS)** field each contain a FAC, press `Cancel`.
   - If the **Auto Alternate Routing (AAR) Access Code** field or the **Auto Route Selection (ARS)** field do not contain a FAC, type a FAC in the field. Select **Enter** to save your changes.

   For more information on Feature Access Codes, including information on how to change or deactivate a FAC, see the Feature Access Code feature description.

Administering the Uniform Dial Plan table

Procedure

1. Enter `change uniform-dial plan` *n*, where *n* is the number of the dial plan that you want to administer.
2. In the **Matching Pattern** field, type the number that you want the software to match to the number that a user dials.
3. In the **Len** field, type the number of digits of the user-dialed number, that the software analyzes when the software compares the user-dialed number with the numbers in the matching pattern field.
4. In the **Del** field, type the number of digits that the software deletes before the software routes a call.

   The number that you type must be less than, or equal to, the number that you type in the **Len** field.
5. In the **Insert Digits** field, type the digits that the software uses to replace the digits that the software deletes from the user-dialed number.

   If you want the software to delete the digits instead of to replace the digits, leave the **Insert Digits** field blank. You can type a maximum of 4 digits.
6. In the **Net** field, type the server or the system network that the software uses to analyze the number that the software converts.

Perform one of the following actions:

- If you want the software to route the converted digit-string as an extension, type `ext`.
- If you want the software to route the converted digit-string as its converted AAR address, type `aar`.
- If you want the software to route the converted digit-string as its converted ARS address, type `ars`.
- If you want the software to route the converted digit-string as its ENP node number, type `enp`.

  If you type `enp`, you must:

  - Type the extension number portability (ENP) node number in the **Node Number** field.
  - Leave the **Insert Digits** field blank. Type `n` in the **Cony** field.

7. In the **Node Num** field, type the ENP node number.
8. In the **Conv** field, perform one of the following actions:
   - If you want additional digit conversion, type `y`.
   - If you do not want additional digit conversion, type `n`.

   Note:

   The **Percent Full** field displays the percent of the allocated uniform dial plan data resources that are currently used. You cannot change this field.
9. Select **Enter** to save your changes.

Administering the Node Number Routing Table for UDP

Procedure

1. Enter `change node-number routing` *n*, where *n* is the number of the node.
2. In the **Route Pat** field, type the number of the routing pattern that you want to use.
3. Select **Enter** to save your changes.

Administering the AAR Digit Conversion Table for UDP

Procedure

1. Enter `change aar digit-conversion` *n*, where *n* is the number of the AAR Digit Conversion Table.

   Note:

   The system sorts the screen information by matching pattern. The software displays numbers first, followed by characters in alphabetical order.
2. In the **Matching Pattern** column, type the number that you want the system to match to the numbers that the user dials.

If you require a prefix digit of 1 for 10-digit DDD, start the matching pattern with a 1.

You can also type `*`, a lower case `x`, or an upper case `X` as wildcard characters.

3. In the **Min** column, type the minimum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column.
4. In the **Max** column, type the maximum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column.
5. In the **Del** column, type the number of digits that you want the system to delete from the beginning of the dialed string.
6. In the **Net** column, type the initials of the call-processing server network that the system uses to analyze the converted number.
7. In the **Conv** column, perform one of the following actions:
   - If you want additional digit conversion, type `y`.
   - If you do not want additional digit conversion, type `n`.
8. Use the **ANI Req** column only if the **Request Incoming ANI (non-AAR/ARS)** field is set to n on the Mutifrequency-Signaling-Related System Parameters screen.

   If the **Request Incoming ANI (non-AAR/ARS)** field is set to n on the Mutifrequency-Signaling-Related System Parameters screen, perform one of the following actions in the **ANI Req** field:
   - If you require ANI on incoming R2-MFC or Russian MF ANI calls, type `y`.
   - If you do not require ANI on incoming R2-MFC or Russian MF ANI calls, type `n`.
   - If the **Allow ANI Restriction on AAR/ARS** field is set to y on the Feature-Related System Parameters screen, type `r`. When you set the **ANI Req** field to r, the system drops a call on a Russian shuttle trunk or a Russian rotary trunk if the ANI request fails. For calls on other types of trunks, the system processes an r entry in the **ANI Req** field as a y.

     The **Percent Full** column displays the percent of the allocated system memory that is used by AAR and ARS. You cannot change this field.
9. Select **Enter** to save your changes.

Administering the ARS Digit Conversion Table for UDP

Procedure

1. Enter `change ars digit-conversion` *n*, where *n* is the number of the ARS Digit Conversion Table.
2. In the **Matching Pattern** column, type the number that you want the system to match to the numbers that the user dials.

   If you require a prefix digit of 1 for 10-digit DDD, start the matching pattern with a 1.

   You can also type `*`, a lower case `x`, or an upper case `X` as wildcard characters.

3. In the **Min** column, type the minimum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column.
4. In the **Max** column, type the maximum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column.
5. In the **Del** column, type the number of digits that you want the system to delete from the beginning of the dialed string.
6. In the **Net** column, type the initials of the call-processing server network that the system uses to analyze the converted number.
7. In the **Conv** column, perform one of the following actions:
   - If you want additional digit conversion, type `y`.
   - If you do not want additional digit conversion, type `n`.
8. Use the **ANI Req** column only if the **Request Incoming ANI (non-AAR/ARS)** field is set to n on the Mutifrequency-Signaling-Related System Parameters screen.

   If the **Request Incoming ANI (non-AAR/ARS)** field is set to n on the Mutifrequency-Signaling-Related System Parameters screen, perform one of the following actions in the **ANI Req** field:
   - If you require ANI on incoming R2-MFC or Russian MF ANI calls, type `y`.
   - If you do not require ANI on incoming R2-MFC or Russian MF ANI calls, type `n`.
   - If the **Allow ANI Restriction on AAR/ARS** field is set to y on the Feature-Related System Parameters screen, type `r`. When you set the **ANI Req** field to r, the system drops a call on a Russian shuttle trunk or a Russian rotary trunk if the ANI request fails. For calls on other types of trunks, the system processes an r entry in the **ANI Req** field as a y.

     The **Percent Full** column displays the percent of the allocated system memory that is used by AAR and ARS. You cannot change this field.
9. Select **Enter** to save your changes.

Administering the AAR Digit Analysis Table for UDP

Procedure

1. Enter `change aar analysis n`, where *n* is the number of the AAR Digit Analysis Table.
2. In the **Dialed String** column, type the numbers that the system compares to the number that the user dials.

   You can also type `*`, a lower case `x`, or an upper case `X` as wildcard characters.

   The system uses the dialed string that most closely matches the number that the user dials. For example, if a user dials 297-1234, and the AAR Digit Analysis Table contains two dialed strings of 297-1 and 297-123, the system uses the dialed string 297-123 as the match.

When the system compares a user-dialed number with an entry in the **Dialed String** column that is an exact match and an entry in the **Dialed String** column with one or more wildcard characters, the system chooses the exact match. For example, if a user dials 424, and the AAR Digit Analysis Table contains two dialed strings of 424 and X24, the system uses the dialed string 424 as the match.

3. In the **Min** column, type the minimum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column.
4. In the **Max** column, type the maximum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column.
5. In the **Route Pattern** column, type the route information that you want the server to use for the dialed string.

   Perform one of the following actions:

   - To specify the route index number that you established on the Partition Routing Table screen, type a value from p1 to p2000.
   - To specify the route pattern that the system uses to route the call, type a number from 1 to 640.
   - To specify the route pattern that the system uses to route the call, type a number from 1 to 999 or 1 to 2000. If you are using the S8300D or S8300E server, you can configure a maximum of 999 route patterns. If you are using the HP DL360 G7, or Dell R610, sever, you can configure a maximum of 2000 route patterns.
   - If RHNPA translations are required for the corresponding dialed string, type a value from r1 to r32 to specify the remote home numbering plan.
   - To designate node number routing, type `node`.
   - To block the call, type `deny`.
6. In the **Call Type** column, type the call type that is associated with each dialed string.

   The call types indicate the numbering requirements on different trunk networks. Perform one of the following actions:

   - For regular AAR calls, type `aar`.
   - If the Route Index contains public network ISDN trunks that require the international type of number encodings, type `intl`.
   - If the Route Index contains public network ISDN trunks that require an unknown type of number encodings, type `pubu`.
   - To specify the ISDN Private Number Plan (PNP) number formats, type `lev0`, `lev1`, or `lev2`.
   - For a UDP numbering plan where extensions are passed (rather than full public network or private-network numbers), type `unku`.

     For more information on ISDN Numbering-Private, see *Administering Avaya Aura® Communication Manager*.

The table on page 1389 describes the ISDN protocols.

Table 125: ISDN protocols

Call type	Numbering plan identifier	Type of numbering
aar	E.164(1)	national(2)
intl	E.164(1)	international(1)
pubu	E.164(1)	unknown(0)
lev0	PNP(9)	local(4)
lev1	PNP(9)	Regional Level 1(2)
lev3	PNP(9)	Regional Level 2(1)
unku	unknown (0)	unkown (0)

7. In the **Node Number** column, type the number of the destination node in a private network if you use node number routing or Distributed Communication System (DCS).
8. Use the **ANI Req** column only if the **Request Incoming ANI (non-AAR/ARS)** field is set to n on the Mutifrequency-Signaling-Related System Parameters screen.

   If the **Request Incoming ANI (non-AAR/ARS)** field is set to n on the Mutifrequency-Signaling-Related System Parameters screen, perform one of the following actions in the **ANI Req** field:

   - If you require ANI on incoming R2-MFC or Russian MF ANI calls, type `y`.
   - If you do not require ANI on incoming R2-MFC or Russian MF ANI calls, type `n`.
   - If the **Allow ANI Restriction on AAR/ARS** field is set to y on the Feature-Related System Parameters screen, type `r`. When you set the **ANI Req** field to r, the system drops a call on a Russian shuttle trunk or a Russian rotary trunk if the ANI request fails. For calls on other types of trunks, the system processes an r entry in the **ANI Req** field as a y.

     The **Percent Full** column displays the percent of the allocated system memory that is used by AAR and ARS. You cannot change this field.
9. Select **Enter** to save your changes.

Administering the ARS Digit Analysis Table for UDP

Procedure

1. Enter `change ars analysis n`,where *n* is the number of the ARS Analysis Table.

   The **location** field is a display-only field.

   - If the **ARS** field and the **Multiple Locations** field on the Optional Features screen are set to y, the **location** field is set to a number between 1 and 250. The numbers 1 through 64 in the **location** field define the location of the server that uses this ARS Digit Analysis Table.
   - If the **ARS** field on the Optional Features screen is set to y, but the **Multiple Locations** field on the Optional Features screen is set to n, the **location** field is set to all. A value

of all in the **location** field indicates that this ARS Digit Analysis Table is the default for all port network locations.

2. In the **Dialed String** column, type the numbers that the system compares to the number that the user dials.

   You can also type `*`, a lower case `x`, or an upper case `X` as wildcard characters.

   The system uses the dialed string that most closely matches the number that the user dials. For example, if a user dials 297-1234, and the AAR Digit Analysis Table contains two dialed strings of 297-1 and 297-123, the system uses the dialed string 297-123 as the match.

   When the system compares a user-dialed number with an entry in the **Dialed String** column that is an exact match and an entry in the **Dialed String** column with one or more wildcard characters, the system chooses the exact match. For example, if a user dials 424, and the AAR Digit Analysis Table contains two dialed strings of 424 and X24, the system uses the dialed string 424 as the match.

3. In the **Min** column, type the minimum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column.
4. In the **Max** column, type the maximum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column.
5. In the **Route Pattern** column, type the route information that you want the server to use for the dialed string.

   Perform one of the following actions:

   - To specify the route index number that you established on the Partition Routing Table screen, type a value from p1 to p2000.
   - To specify the route pattern that the system uses to route the call, type a number from 1 to 640.
   - To specify the route pattern that the system uses to route the call, type a number from 1 to 999. Use this number range only for the S8XXX Server.
   - If RHNPA translations are required for the corresponding dialed string, type a value from r1 to r32 to specify the remote home numbering plan.
   - To designate node number routing, type `node`.
   - To block the call, type `deny`.

6. In the **Call Type** column, type the call type that is associated with each dialed string.

   The call types indicate the numbering requirements on different trunk networks. Perform one of the following actions:

   - To alert attendant consoles or other digital telephones when a user places an emergency call, type `alrt`.

     This call type is a normal China number 1 call type.

- To designate an emergency call, type `emer`.

  This call type is a normal China number 1 call type.
- To designate a 10-digit North American Numbering Plan (NANP) call, type `fnpa`. NANP calls consist of 11 digits and a prefix digit of 1.

  This call type is an attendant China number 1 call type.
- To designate a 7-digit NANP call, type `hnpa`.

  This call type is a normal China number 1 call type.
- To designate a public network international number, type `intl`.

  This call type is a toll-auto China number 1 call type.
- To designate an international operator, type `lop`.

  This call type is an attendant China number 1 call type.
- To designate a non-NANP call, type `natl`.

  This call type is a normal China number 1 call type.
- To designate a national private call, type `npvt`.

  This call type is a normal China number 1 call type.
- To designate a national service call, type `nsvc`.

  This call type is a normal China number 1 call type.
- To designate an operator call, type `op`.

  This call type is an attendant China number 1 call type.
- To designate a public network number (E.164) unknown call, type `pubu`.

  This call type is a normal China number 1 call type.
- To designate a national(2) call, type `svcl`.

  This call type is a toll-auto China number 1 call type.
- To designate a national(2) call, type `svct`.

  This call type is a normal China number 1 call type.
- To designate a service call, first part control, type `svft`.

  This call type is a local China number 1.
- To designate a service call, first part control, type `svfl`.

  This call type is a toll China number 1 call type.

7. In the **Node Number** column, type the number of the destination node in a private network if you use node number routing or DCS.
8. Use the **ANI Req** column only if the **Request Incoming ANI (non-AAR/ARS)** field is set to n on the Mutifrequency-Signaling-Related System Parameters screen.

If the **Request Incoming ANI (non-AAR/ARS)** field is set to n on the Mutifrequency-Signaling-Related System Parameters screen, perform one of the following actions in the **ANI Req** field:

- If you require ANI on incoming R2-MFC or Russian MF ANI calls, type `y`.
- If you do not require ANI on incoming R2-MFC or Russian MF ANI calls, type `n`.
- If the **Allow ANI Restriction on AAR/ARS** field is set to y on the Feature-Related System Parameters screen, type `r`. When you set the **ANI Req** field to r, the system drops a call on a Russian shuttle trunk or a Russian rotary trunk if the ANI request fails. For calls on other types of trunks, the system processes an r entry in the **ANI Req** field as a y.

  The **Percent Full** column displays the percent of the allocated system memory that is used by AAR and ARS. You cannot change this field.

9. Select **Enter** to save your changes.

Administering the extension number portability numbering plan

Procedure

Enter `change enp-number-plan`.

For more information on the Extension Number Portability Numbering Plan screen, see *Administering Network Connectivity on Avaya Aura® Communication Manager*.

Reports for Uniform Dial Plan

The following reports provide information about the Uniform Dial Plan capability:

- The Uniform Dial Plan report shows the details of the Dial Plan.

For detailed information on these reports and the associated commands, see *Avaya Aura® Communication Manager* Reports.

Considerations for Uniform Dial Plan

This section provides information about how the Uniform Dial Plan (UDP) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Uniform Dial Plan under all conditions.

- In North American network environments, the system routes extensions that start with 0 to an attendant. Avaya recommends that you use a digit other than 0 as the leading digit when you assign extensions.

- When you call an extension that is on another server, you might experience slight delay before you hear call-progress tones. This delay is caused by the trunk signaling that is necessary to complete the call to the remote media server or to the switch.
- When you select the option that causes the software to look at the UDP table first, the system routes calls that might otherwise terminate at a local extension, over the network. If you do not want the system to route calls over the network, you must remove the extensions from the UDP table. Once you remove the extensions from the UDP table, users can dial the local extension.
- If Automatic Alternate Routing (AAR) is active, the software sends facility restriction levels (FRLs) and Traveling Class Marks (TCMs) with the private network number. UDP Code and AAR Code conversions use the FRL that is assigned to the caller. Extension number portability (ENP) Node conversion always raises the FRL to the maximum of seven.

  If an FRL is insufficient to access the facility, the system denies access. The system does not prompt for an authorization code, even if authorization codes are enabled and administered in your system.
- If AAR is inactive, do not equip your system to use tandem-tie trunks to transport UDP numbers. You should not use tandem-tie trunks to transport UDP numbers, because the termination server does not recognize the TCM.

  Avaya recommends that you never use tandem-tie trunks to transport UDP numbers. When you use tandem-tie trunks to transport UDP numbers, the receiving media server or the system does not recognize the TCM and the hop count that follow the extension.

Interactions for Uniform Dial Plan

This section provides information about how the Uniform Dial Plan (UDP) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Uniform Dial Plan in any feature configuration.

Automatic Alternate Routing (AAR)

AAR routes UDP calls. The AAR subset is included with the UDP. If AAR and UDP are both enabled on your system, the 7-digit AAR number provides the same routing as the UDP.

Dial Plan

- Extension numbers on a server do not need to be part of a UDP. When extension numbers are not part of a UDP, the server software uses a non-UDP to handle calls that are associated with those extensions.
- When you administer the Dial Plan and designate a group of extensions as UDP nonlocal, you can specify either that the software search for local extensions first, or search for local extensions last.

Direct Inward Dialing (DID) trunk group

DID calls to a UDP extension number might require the DID trunk group to insert the necessary digits to create the full extension number. For example, if the DID trunk provides 4 digits, but a 5-digit UDP is in place, the DID trunk group must insert the appropriate leading digit.

Distributed Communications System (DCS)

UDP is required when DCS is provided. The necessary UDP software is provided with the DCS software.

Extension Number Portability (ENP)

If you administer a user extension to use ENP node routing, ENP routes the call to the correct server.

If you enable both AAR and UDP, the 7-digit AAR number provides the same routing as UDP. The 7-digit AAR number uses ENP to route the call.

Chapter 185: Visually Impaired Attendant Service

Use the Visually Impaired Attendant Service (VIAS) feature to provide voice feedback to a visually impaired attendant. Each voice phrase is a sequence of one or more single-voiced messages.

Detailed description of Visually Impaired Attendant Service

Visually Impaired Attendant Service (VIAS) defines six buttons for the visually impaired attendant:

- Visually impaired service activation and deactivation

  This button activates or deactivates VIAS. When you press the button, the system re-enables all ringers that are disabled, such as the recall and incoming call ringers.

- Console status

  When you press this button, the system provides voice feedback of the status of the:

  - Console, for example, busy, available, or night service
  - Attendant queue
  - System alarms

- Display status

  When you press this button, the system provides voice feedback of the information that is on the console display. VIAS is unavailable for some displays, such as Class of Restriction (COR), restriction information, personal names, and the purpose of some calls.

- Last operation

  When you press this button, the system provides voice feedback of the last operation that was performed at the console.

- Last voice message

  When you press this button, the system provides voice feedback of the most recent message at the console.

- Direct trunk group selection status

When you press this button, the system provides voice feedback of the status of an attendant-monitored trunk group.

A visually impaired attendant can use the Inspect mode to locate each button, to determine the feature that is assigned to the button.

Visually Impaired Attendant Service administration

This section contains prerequisites and the screens that you use to administer the Visually Impaired Attendant Service (VIAS) feature.

Preparing to administer Visually Impaired Attendant Service

Procedure

Set up an attendant console.

For information on how to set up an attendant console, see the *Administering Avaya Aura® Communication Manager*.

Screens for administering Visually Impaired Attendant Service

Screen name	Purpose	Fields
Attendant Console	Administer the Visually Impaired Attendant Service (VIAS) buttons: • vis • con-stat • display • dtgs-stat • last-mess • last-op	Any available button field in the **Feature Button Assignments** area

Interactions for Visually Impaired Attendant Service

This section provides information about how the Visually Impaired Attendant Service (VIAS) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Visually Impaired Attendant Service (VIAS) in any feature configuration.

Audible Message Waiting

The system generates a stutter tone before the dial tone, when a message waits at an extension. A visually impaired attendant can use the stutter tone, instead of a message light, to detect a message that waits at an extension.

Auto Start and Don’t Split

If you activate or deactivate VIAS while Auto Start and Don’t Split is active, the system deactivates Auto Start and Don’t Split.

Automatic Circuit Assurance (ACA)

When the attendant presses the display button, the system provides the following voice messages:

- “Automatic Circuit Assurance,” if an ACA call is unanswered
- “Automatic Circuit Assurance,” and the extension that is assigned to the ACA call, if the call is answered

Malicious Call Trace (MCT)

The system provides voice feedback of the displays that are related to MCT activation, but not of the displays that are related to MCT control.

Chapter 186: Voice Message Retrieval

Using the Voice Message Retrieval feature, you can allow attendants, telephone users, and remote users to retrieve Leave Word Calling (LWC) messages and Call Coverage messages.

Detailed description of Voice Message Retrieval

Voice Message Retrieval is used only for the retrieval of messages. When a telephone is in Voice Message Retrieval mode, you cannot use the telephone to make calls or access other features. You can use Voice Message Retrieval to retrieve your own messages, or messages for another user. However, a different user's messages for another user can only be retrieved at a telephone or an attendant console that is in the coverage path. This is done by an administered system-wide message retriever, or by a remote-access user when the extension and the associated security code are known.

You can designate certain telephones and attendants for system-wide message retrieval. These telephones are the same as that you use for Display Message Retrieval, and have the same privileges. Voice Message Retrieval cannot be accessed from rotary telephones.

You can restrict unauthorized users from retrieving messages. Use the Lock function to restrict a telephone and the Unlock function to release the restriction. To activate Lock, users dial a system-wide access code. To cancel Lock, users dial a system-wide access code, and then an Unlock security code that is unique to the telephone. These functions only apply to the telephone where the function is active. The system-wide access codes and security code that you use for the Lock and Unlock functions are the same as those use for LWC message retrieval by display. You can assign a status lamp to show the Lock status of the telephone.

Voice Message Retrieval administration

This section describes the screens that you use to administer the Voice Message Retrieval feature.

Screens for administering Voice Message Retrieval

Screen name	Purpose	Fields
Feature Access Code (FAC)	Set up Voice Message Retrieval.	• LWC Message Retrieval Lock • LWC Message Retrieval Unlock • Voice Coverage Message Retrieval Access Code • Voice Principal Message Retrieval Access Code
Feature Related System Parameters	Administer Voice Message Retrieval.	• Stations With System-Wide Retrieval Permission Message • Waiting Lamp Indicates Status
Station	Set up Voice Message Retrieval.	Security Code

Interactions for Voice Message Retrieval

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

Communication Manager Messaging Interface

Retrieval of Leave Word Calling (LWC) messages by way of Voice Message Retrieval is separate and distinct from retrieval of messages by way of Communication Manager Messaging. You cannot use Voice Mail Retrieval to access LWC messages on Communication Manager Messaging. However, the user who calls Voice Message Retrieval is informed of any new messages for the principal on Communication Manager Messaging:

- The Voice Message Retrieval voices that there are messages on the Communication Manager Messaging system.
- The Display Message Retrieval displays “Message Center AUDIX Call.”

Bridged Call Appearance

Voice Message Retrieval on a Bridged Call Appearance functions the same as if the feature were activated by the primary extension that is associated with the bridged call appearance.

Leave Word Calling (LWC)

Any authorized touchtone telephone user can retrieve messages by LWC enhanced by Voice Message Retrieval.

Chapter 187: V.150.1 Modem-over-IP

Communication Manager supports the industry standard Modem-over-IP (MoIP) to interoperate with secure terminals and third-party SIP gateways. Modem-over-IP uses the Simple Packet Relay Transport (SPRT) protocol to transmit data packets between modem devices.

Modem devices use the V.150.1 protocol to transmit V-series modem signals between modems and telephony devices. The V.150.1 protocol is a standard recommended by International Telecommunication Union (ITU) to use a modem over IP networks that support dialup modem calls. The V.150.1 protocol defines how to transmit modem traffic between modems and telephony devices over an IP network.

With the Modem-over-IP feature, secure terminals establish a secured connection over SIP and H.323 trunks and the Avaya proprietary Inter-gateway Connections (IGCs).

The Modem-over-IP feature operates only with:

- G450 gateways that use the new DAR4 card, also known as MP160
- Media Gateways Release 6.2 and later

Related links

Detailed description of V.150.1 Modem-over-IP on page 1400

Detailed description of V.150.1 Modem-over-IP

Communication Manager 6.2 and earlier used pass-through and relay modes for modem transport. Only the following Avaya gateways support the protocols used for the earlier modem transport modes: G430, G450. These methods did not work well with all modem terminals. V.150.1 Modem-over-IP feature implements modem features according to the V-series industry standard to interoperate with non-Avaya modem equipment, trunk-side and line-side, for end-to-end secure connections over IP. V.150.1 specifies a protocol for transport of end-to-end modem signals, for devices designed to transport V-series modem signals across an IP network. This feature provides a connection path between two modems such that the modem signals are fully terminated in the gateway.

Related links

V.150.1 Modem-over-IP on page 1400

V.150.1 Modem-over-IP administration

Screens for administering V.150.1 Modem-over-IP

Screen name	Purpose	Fields
IP codec set	Administering the **V.150.1 Modem-over-IP** feature	**Modem mode**

Related links

V.150.1 Modem-over-IP on page 1400

Administering V.150.1 Modem-over-IP

Procedure

1. Type `change ip-codec-set n`, where *n* is the Codec Set number.
2. On page 2 of the IP Codec Set screen, set the **Modem** field to v150mr.

   The system displays the V.150 MODEM RELAY PARAMETERS page.

   Note:

   On the V.150 MODEM RELAY PARAMETERS page, the default settings are applicable for any V.150.1 implementation, so you need not change the values.
3. Save the changes.

Related links

V.150.1 Modem-over-IP on page 1400

Chapter 188: Whisper Paging

Using the Whisper Paging feature, one user can interrupt or barge in on the call of another user and make an announcement. The paging user dials a Feature Access Code (FAC) or presses a feature button, and then dials the extension of the other user.

Detailed description of Whisper Paging

With the Whisper Paging feature, the page is unique because only the person on the paged extension can hear the page. Other parties on the call cannot hear the page, and the person who makes the page cannot hear anyone on the call. If the paged user has a display telephone, the paged user can see who makes the whisper page.

For example, users A and B are on a call. User C has an urgent message for user A and makes a whisper page. All three users hear the tone that signals the page, but only user A hears the page itself. User who make the page cannot hear users A or B.

Whisper Paging call redirection overrides

If a paged user is not on an active call, a whisper page is converted to a priority call that overrides any of the following call redirection features:

- Call Forward All Calls
- Call Forward Busy
- Call Forward Don’t Answer
- Send All Calls
- Go To Cover
- Call Coverage

For example, if Call Forward All Calls is activated on a telephone on which no active calls exist, a whisper page to that telephone rings as a priority call.

Whisper Paging in Group answering environments

Whisper Paging does not work with extensions that are assigned to a group answering environment. You cannot place a whisper page to the main extension that is assigned to a hunt

group, a split, a skill, or a terminating extension group (TEG). You cannot place a whisper page to any extension that is a member of one of these groups.

Whisper Paging network restrictions

Whisper Paging does not work across networks, such as Distributed Communication System (DCS) networks or electronic tandem networks. Both the paging user and the paged user must be on the same server that runs Communication Manager.

Whisper Paging with speakerphones

When a call is on the speaker, an incoming whisper page is also heard over the speaker too. When the group listening feature on a 6400-series telephone is active, an incoming whisper page is heard on both the handset and the speaker.

Whisper Paging administration

The following tasks are part of the administering process for the Whisper Paging feature:

- Activating Whisper Paging
- Allowing users to answer whisper pages quickly
- Allowing users to block whisper pages

Related links

Activating Whisper Paging on page 1403
Allowing users to answer whisper pages quickly on page 1404
Allowing users to block whisper pages on page 1404

Screens for administering Whisper Paging

Screen name	Purpose	Fields
Station	Activate Whisper Paging buttons.	• Whisper Page Activation • Answerback • Whisper Page Off
Feature Access Code (FAC)	Activate a FAC to Whisper Page.	Whisper Page Activation Access Code

Activating Whisper Paging

Procedure

1. To assign a Feature Access Code, enter a code in the **Whisper Page Activation Access Code** field on the Feature Access Code screen.

2. To give users a feature button for making a whisper page, use the Station screen and administer a **Whisper Page Activation** button on users' telephones.

Allowing users to answer whisper pages quickly

About this task

To give users a feature button for answering a whisper page, use the Station screen and administer an **Answerback** button on users' telephones.

Note:

You cannot administer an **Answerback** button on an attendant console. Attendants can make whisper pages but cannot receive them.

Normally, before a paged user can answer a whisper page, he or she must complete the active call or put it on hold. However, you can give users the ability to put an active call on hold and speak directly to the person making a whisper page simply by pushing a feature button. Once the **Answerback** button is pressed, the user can treat both the paging call and the original call as separate calls and all call-related features (conference, transfer, and so on) operate normally.

Allowing users to block whisper pages

About this task

To give users a feature button to block incoming whisper pages, use the Station screen and administer a **Whisper Page Off** button on users' telephones.

Administer this function on a feature button with a lamp so that users can tell whether blocking is active or inactive. Users can activate blocking even when they are on a call.

Note:

You cannot administer a **Whisper Page Off** button on a soft key.

The Do Not Disturb and Privacy - Attendant Lockout features can also block incoming whisper pages.

End-user procedures for Whisper Paging

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.

To make a whisper page, users dial a FAC or press a feature button, then dial the extension of the user they are trying to reach.

Considerations for Whisper Paging

This section provides information about how the Whisper Paging feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Whisper Paging under all conditions. The following considerations apply to Whisper Paging:

- The Whisper Page feature currently does not work correctly if each of the call's parties is using a SIP endpoint administered on and managed by a different instance of Communication Manager.

Interactions for Whisper Paging

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

Attendant

Attendants cannot intrude on a whisper page. If an attendant is using intrusion to talk to a user, that user cannot receive a whisper page.

An attendant can use auto-manual splitting to start a whisper page. However, the attendant cannot use Release, Hold, or Split after the page is made.

Bridged Call Appearances

Whisper pages are designed to reach a specific user associated with a specific extension.

- When an extension and one or more of its bridged appearances are in use, parties on the bridged appearances hear the tone that signals an incoming whisper page but only the user on the principle extension hears the announcement. Only the display on the principle extension shows the whisper page message.
- When all appearances are idle or only a bridged appearance is in use, a whisper page rings the principal extension with priority ringing.
- If a user makes a whisper page on a call appearance that is a member of a bridge group, then no others users in the bridge group can connect to the call while the whisper page intrusion is active.

Busy Verification

You can’t make a whisper page to an extension while it’s being busy-verified. You cannot busy-verify an extension while it’s making or receiving a whisper page.

Calling Restrictions - Origination

Telephones with this restriction cannot make whisper pages.

Calling Restrictions - Termination

Telephones with this restriction cannot receive whisper pages.

Class of Restriction (COR)

A station user must have a COR for station-to-station calling to perform Whisper Paging to a member outside of their own COR. Calling and called party restrictions also determine which extensions can make and receive whisper pages.

Conference

If a user is on a conference call and starts a whisper page, everyone on the conference call hears the tone that signals the page. However, only the owner of the paged extension hears the page message and the user making the whisper page is dropped from the conference call. For example, A is on a conference call at the first call appearance. A puts the call on hold and starts a whisper page from the second call appearance to B. B hears the whisper page. However, A is dropped from the conference call, which is held at the first call appearance.

The system does not update the display of the paging and the paged extensions. The telephone of the person who makes the page displays the whisper page to the paged extension. The paged extension displays the conference call. Only the display of the other parties in the conference call gets updated. The extension shows the parties active on the conference call. For example, if A, B, and C are in conference and A makes a whisper page to B, A displays the whisper to B, B displays the conference call, and C displays the name and the number of B.

If a conference call already has the maximum number of parties and trunks, you cannot make a whisper page to any of the participants. If an active whisper page is on the call, you cannot add parties to a conference call.

Data Privacy - Permanent or Temporary

Any station that has Data Privacy activated cannot make a whisper page.

Data Restriction

A whisper page to a station is denied when Data Restriction is enabled on a station or trunk.

Expert Agent Selection

You cannot make a whisper page by dialing an agent’s Logical Agent ID. Pages must be made to a physical extension.

Go to Cover

If you make a whisper page and then press your **Go To Cover** button while the page is in progress, the **Go To Cover** button does not work. The opposite is true as well. If you activate Go to Cover and press the whisper page activation button, you cannot make a whisper page.

Last Number Dialed

When you make a whisper page, the page is tracked as the last number dialed.

QSIG

This feature does not operate in a QSIG environment.

Remote Access

You cannot make a whisper page by remote access. Both the paging party and the paged party must be on the same media server or the attempt is denied.

Service Observing

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

Tenant Partitioning

Whisper paging is permitted across tenant partitions if the assigned classes of restriction support intercom calling between members of different partitions. This feature is especially useful to attendants who serve multiple partitions.

Note:

System administrators must ensure that this feature is managed appropriately in systems with tenant partitioning. Some tenants might not want other tenants to interrupt their calls.

Transfer

A call cannot be transferred during an active whisper page.

Vector Directory Number (VDN)

You cannot make a whisper page to a VDN. Pages must be made to a physical extension.

Chapter 189: World Class Routing

Use the World Class Routing feature to direct outgoing calls. The World Class Routing feature has two capabilities, Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS).

- Automatic Alternate Routing (AAR) routes calls within your company over your own private network.

  The system converts the number that the user dials. The system then analyzes the number, and routes the call as a private-network call.

- Automatic Route Selection (ARS) routes calls that go outside your company over public networks. ARS also routes calls to remote company locations if you do not have a private network.

  The system converts the number that the user dials. The system then analyzes the number, and routes the call as a public network call.

Automatic routing starts when a user dials a Feature Access Code (FAC) and then the number that the user wants to call. The system analyzes the dialed digits, selects the route for the call, and deletes and inserts digits, if necessary. The system then routes the call over the trunks that you specify in your routing tables. AAR and ARS can access the same trunk groups, and share the same route patterns and other routing information. ARS calls can be converted to AAR calls, and AAR calls can be converted to ARS calls.

The FAC for AAR is usually the digit 8. The FAC for ARS is usually the digit 9 in the US and 0 outside the US. When your Avaya technician or business partner sets up AAR on your server that is running Communication Manager, he or she usually assigns the FAC for AAR. You can administer your own FAC for ARS. With Communication Manager 2.0, you can also use ARS without a FAC.

Detailed description of World Class Routing

Automatic routing starts when a user dials a Feature Access Code (FAC) and then the number that the user wants to call. The system analyzes the dialed digits, selects the route for the call, and deletes and inserts digits, if necessary. The system then routes the call over the trunks that you specify in your routing tables. AAR and ARS can access the same trunk groups, and share the same route patterns and other routing information. ARS calls can be converted to AAR calls, and AAR calls can be converted to ARS calls.

The FAC for AAR is usually the digit 8. The FAC for ARS is usually the digit 9 in the US and 0 outside the US. When your Avaya technician or business partner sets up AAR on your server

that is running Communication Manager, he or she usually assigns the FAC for AAR. You can administer your own FAC for ARS. With Communication Manager 2.0, you can also use ARS without a FAC.

Overview of automatic routing

The following figure shows an overview of automatic routing:

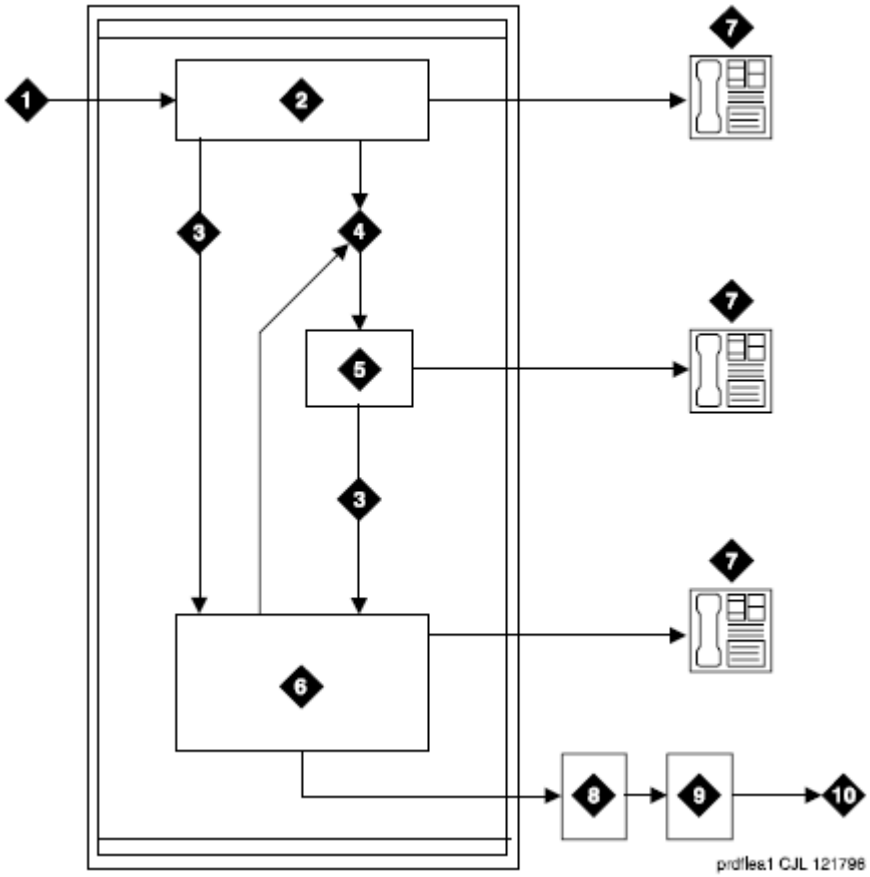


Figure 34: Automatic Routing Overview

Number	Description
1	Receive input from a telephone, a public network trunk, or a private network trunk.
2	Analyze the digits to determine the address type from the Dial Plan Analysis Table.
3	Direct the call to Automatic Alternate Routing (AAR) or Automatic Route Selection (ARS).
4	Direct the call to the Uniform Dial Plan (UDP).
5	Use the UDP to determine the route.

Table continues…

Number	Description
6	Delete and insert digits based on the ARS Digit Analysis Table.
7	Terminate the call at the telephone.
8	Analyze the digits based on information from the ARS Digit Analysis Table. Determine the route pattern.
9	Select an outgoing trunk group and delete and insert digits.
10	Send the call to a public network trunk or a private network trunk.

ARS analysis description

With ARS, the system checks the digits in the called number against an ARS Digit Analysis Table to determine how to handle the dialed digits. The system also uses Class of Restriction (COR) and Facility Restriction Level (FRL) to determine the calling privileges.

- Dialed string. Lists the first digits in the dialed string. When a user makes an outgoing call, the system analyzes the digits, and looks for a match in the table. The system then uses the information in the matching row to determine how to route the call.

  For example, if a caller places a call to 1-303-233-1000, the system matches the dialed digits with the digits in the first column of the table. In this example, the dialed string matches the digit 1. Then the system matches the length of the entire dialed string (11 digits) to the minimum (Min) and the maximum (Max) length columns. In this example, the 11-digit call that started with 1 follows route pattern 30 as an fnpa call.

  The first dialed digit for an external call is often an access code. If the digit 9 is defined as the ARS access code, the system drops this digit and uses the ARS Analysis Table to analyze the remaining digits.
- Route Pattern. Indicates the route that handles the calls that match the dial string.
- Call Type. Describes what kind of call is made with this dial string. Call Type helps the system determine how to handle the dialed string.
- Node Num. States the number of the destination node in a private network, if you use node number routing or Distributed Communication System (DCS). Valid values are 1 to 999, or blank.

For more information, see *Administering Avaya Aura® Communication Manager*.

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).

Table continues…

Operation	Actual Digits Dialed	Matching Pattern	Replacement String	Modified Address	Notes
International call to announcement (This method can also be used to block unauthorized IDDD calls)	9-011-91-672530	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.

ARS dialing without a FAC

Using this feature, users can place calls without the need to first dial a Feature Access Code (FAC), such as the number 9, to access an outside line. The system recognizes the call as an ARS or an AAR call, and accordingly uses the ARS or the AAR digit analysis and digit conversion tables to route the call. This enhancement was added to the Communication Manager Release 2.0.

This feature provides for the following additional calling options:

- Public network dialing. This feature eliminates the need to enter a FAC to gain access to a public network facility or trunk. The typical application is apartments or assisted living complexes that want to provide the sense that users can directly dial the public network.
- UDP networks. Many customers have large networks with 5-digit UDPs that have that have “run out of numbers”. With this feature, you can extend the network dial plan. The DCS feature transparency is available only with 4-digit and 5-digit dialing plans.
- QSIG networks. The QSIG implementation does not require a 4-digit or a 5-digit UDP like DCS. An expanded private-network dial plan makes it easier to integrate the system into existing customer enterprise networks that are made up of non-Communication Manager systems. An expanded dial plan also facilitates those customers who want to convert a large DCS network to QSIG signaling protocol. DCS is not supported for private-network dial plans that are greater than 5-digits.
- 3-Digit UDP. ARS dialing without a FAC enables 3-digit UDP. However, DCS does not work in a dial scheme of less than 4 digits. For feature transparency, QSIG must be used for signaling.

Avaya recommends that you use ARS or AAR Dialing without a FAC only when users dial outside central office (CO) trunks. If you use this feature to expand dial plan lengths beyond 7-digits for

internal extensions across a private QSIG or DCS network, some feature interactions might occur. Such interactions can include changes in the information that is shown on display telephones, telephony features, and call center features. ARS and AAR Dialing without a FAC is not tested against all possible feature interactions in an intraswitch networked environment. Avaya does not recommend ARS and AAR Dialing without a FAC for this use.

Extension restrictions with World Class Routing

A dialable extension is an extension that is can be dialed without going through ARS or AAR routing.

A nondialable extension is an extension that can only be dialed using ARS or AAR routing. You cannot dial a nondialable extension as it is administered. You must dial a nondialable extension with a prefix as a longer number than the administered extension.

An internal extension is an extension of up to 16 digits.

Use the following general rules to determine how nondialable extensions interact with a particular feature:

- When a user dials an extension directly from a telephone, or the system dials an extension when a feature is invoked, the ARS or AAR Dialing without a FAC feature must be used.
- When a feature, such as Coverage Paths or Security Violation Notification (SVN), is being administered on behalf of a telephone user, the internal extension must be entered through the administration tool.

AAR and ARS partitioning

You can use AAR and ARS partitioning to change the call routing plan for up to eight different user groups on a single server that is running Communication Manager. You assign a Partition Group Number (PGN) to each user group and identify different call routing treatment for each PGN.

For example, you can partition hotel employees and guests into separate groups and route the calls differently. When a guest makes a long distance call, the guest's PGN and digit analysis tables route the call to a telephone billing system that allocates long distance charges. The system routes a similar call placed by an employee over a DDD trunk.

Partition user groups are used only with AAR, ARS, and UDP. You can assign AAR and ARS partitioning to telephones, attendant consoles, remote-access users, data endpoints, and incoming trunks.

Use partitioning for:

- Groups that have different routing because of special billing needs
- Groups that have dedicated use of a particular network facility
- Groups in different businesses that are serviced by a single system
- Data users who require special facility types on outgoing calls

You can assign a route pattern to just one partitioned user group, or you can assign a route pattern to all partitioned user groups.

World Class Routing administration

The following tasks are part of the administration process for World Class Routing:

- COR and FRL World Class Routing administration
- Assigning a FAC for ARS
- Setting up a location ARS FAC
- Displaying ARS analysis information
- Route pattern administration
- Defining call types
  - Defining operator-assisted calls
  - Defining interexchange carrier calls
- Using restricted area codes and prefixes
- Using wildcards
- Defining local information calls
- Modifying call routing
  - Adding a new area code
  - Adding a new prefix
  - Using ARS to restrict outgoing calls
- ARS partition definition
  - Setting up partition groups example
  - Assigning a telephone to a partition group
- Time of Day Routing administration

Related links

COR and FRL World Class Routing administration on page 1415
Assigning a FAC for ARS on page 1416
Setting up a location ARS FAC on page 1417
Displaying ARS analysis information on page 1417
Route pattern administration on page 1417
Defining call types for World Class Routing on page 1426
Using restricted area codes and prefixes for World Class Routing example on page 1427
Using wildcards for World Class Routing example on page 1428
Defining local information calls for World Class Routing example on page 1428
Modifying call routing on page 1429
ARS partition definition on page 1431
Time of Day Routing administration on page 1433

Screens for administering World Class Routing

Screen name	Purpose	Fields
Station	Change the calling privileges of a telephone.	COR
Locations	Create a location ARS Feature Access Code (FAC).	ARS Prefix 1 Required For 10-Digit NANP Calls
AAR and ARS Digit Analysis Table	Define call types and interexchange carrier calls.	Dialed String
ARS Digit Analysis Table	Use wild cards.	• Dialed String • Total Min and Total Max • Route Pattern • Call Type
ARS Digit Analysis Table	Define local information calls.	• Dialed String • Total Min and Total Max • Route Pattern • Call Type
• ARS Chosen Report • ARS Digit Analysis Table	Add a new area code or a prefix.	• Total Min and Total Max • Route Pattern • Call Type • Node Num
ARS Digit Analysis Table	Restrict outgoing calls.	• Dialed String • Total Min and Total Max • Route Pattern • Call Type
• ARS Chosen Report • Partition Routing Table	Set up partition groups.	• Route Pattern • PGN
• Class of Restriction Information • Authorization Code-COR Mapping	Assign a telephone to a partition group.	• COR description • Partition Group Number
Time of Day Routing Plan	Set up time of day routing.	• All • PGN

COR and FRL World Class Routing administration

Each time that you set up a telephone, you use the Station screen to assign a Class of Restriction (COR). You can create different CORs for different groups of users. For example, you might want executives in your company to have different calling privileges than receptionists.

When you set up a COR, you specify a facility restriction level (FRL) on the Class of Restriction screen. The FRL determines the calling privileges of the user. FRLs are ranked from 0 to 7, where 7 has the highest level of privileges.

You also assign an FRL to each route pattern preference on the Route Pattern screen. When a user makes a call, the system checks the COR of the user. The call is allowed if the FRL of the caller is higher than or equal to the FRL of the route pattern preference.

Suppose that you are setting up a telephone for a new executive. The current translations assign COR 1, with outward restrictions and an FRL of 0, which is the lowest permission level available. You want to assign a COR with the highest level of permissions, FRL 7.

Changing the COR of a station for World Class Routing calling privileges

Procedure

1. Enter `change station n`, where *n* is the extension.
2. In the **COR** field, type the number of the new COR.
3. Select **Enter** to save your changes.

Changing the FRL of a COR for World Class Routing calling privileges

Procedure

1. Enter `change cor n`, where *n* is the COR that you want to change.
2. In the **FRL** field, type the number of the new FRL.
3. Select **Enter** to save your changes.

Assigning a FAC for ARS

About this task

To access the public network from an extension in your internal system, a FAC for ARS must be set up on your system. In the US, the number 9 is usually the ARS FAC to use to make an outgoing call.

Procedure

1. Enter `change dialplan analysis`.
2. In an empty row, type the number in the **Dialed String** column that you want to use as the FAC for ARS.
3. In the **Total Length** column, type the total number of digits for the FAC for ARS.
4. In the **Call Type** column, type `fac`.
5. Select **Enter** to save your changes.
6. Enter `change features-access-codes`.
7. In the **Auto Route Selection (ARS) Access Code 1** field, type the number that you set up in Step 2.

8. Select **Enter** to save your changes.

Setting up a location ARS FAC

Before you begin

On the Optional Features screen, ensure that the **Multiple Locations** field is set to `y`.

- If this field is set to y, you can administer up to 250 locations depending on the configuration of the server that is running Communication Manager.
- If the **Multiple Locations** field is set to n, information for Location No. 1 applies to all your locations.

To view the Optional Features screen, type `display system-parameters customer-options`.

Procedure

1. Enter `change locations`..
2. In the **ARS Prefix 1 Required For 10-Digit NANP Calls** field, type `y`.
3. Select **Enter** to save your changes.

Note:

The system uses the ARS access code on the Feature Access Code (FAC) screen when a location ARS does not exist. If a location ARS FAC exists, the ARS access code on the Feature Access Code (FAC) screen is denied from that location. If you use a local ARS code, the ability to administer two ARS codes on the Feature Access Code (FAC) screen is lost.

Displaying ARS analysis information

Procedure

1. Enter `display ars analysis` *n*, where *n* is the first number or numbers of the dialed string that you want to review.

Note:

The system displays only as many dialed strings as can fit on one screen at a time.

2. Select **Enter** to exit the screen.

Important:

To see all the dialed strings that are defined for your system and run an ARS Digit Analysis report: Enter `list ars analysis`.

Route pattern administration

The Route Pattern screen defines the route patterns that the server uses. Each route pattern contains a list of trunk groups that can be used to route the call. The maximum number of route

patterns and trunk groups allowed depends on the configuration and the memory that is available on the system.

Use this screen to insert or delete digits so that the system routes AAR or ARS calls over different trunk groups. You can convert an AAR number into an international number, and insert an area code in an AAR number to convert an on-network number to a public network number. Also, when a call directly accesses a local central office (CO), if the long-distance carrier provided by your CO is unavailable, the system can insert the dial access code for an alternative carrier into the digit string.

Administering the route pattern

Procedure

1. Enter `change route-pattern n`, where *n* is the number of the route pattern.

   Important:

   The next step is for US customers only.

2. In the **Band** field, type a number that represents the OUTWATS band number.

   WATS is a voice-grade service that provides both voice and low-speed data transmission calls to defined areas, or bands, for a flat rate charge.

   The system displays the **Band** field when the **Services/Features** field is set to outwats-bnd, and when either the **ISDN-PRI** or **ISDN-BRI Trunks** field is set to y on the Optional Features screen. The **Band** field is required by Call-by-Call Service Selection.

3. In the **BBC Value** (Bearer Capability Class) area, type the following information in the corresponding columns.

   The columns are labeled **0**, **1**, **2**, **3**, **4**, and **W**.

   - In the **0** column, perform one of the following actions:
     - If the BCC is appropriate for the associated route pattern, type `y`.
     - If the BCC is not appropriate for the associated route pattern, type `n`.
   - In the **1** column, perform one of the following actions:
     - If the BCC is appropriate for the associated route pattern, type `y`.
     - If the BCC is not appropriate for the associated route pattern, type `n`.
   - In the **2** column, perform one of the following actions:
     - If the BCC is appropriate for the associated route pattern, type `y`.
     - If the BCC is not appropriate for the associated route pattern, type `n`.
   - In the **3** column, perform one of the following actions:
     - If the BCC is appropriate for the associated route pattern, type `y`.
     - If the BCC is not appropriate for the associated route pattern, type `n`.

- In the **4** column, perform one of the following actions:
  - If the BCC is appropriate for the associated route pattern, type `y`.
  - If the BCC is not appropriate for the associated route pattern, type `n`.
- In the **W** column, perform one of the following actions:
  - If the BCC is appropriate for the associated route pattern, type `y`.
  - If the BCC is not appropriate for the associated route pattern, type `n`.

  Information in the **BCC Value** area identifies the type of call that is appropriate for this trunk group, such as voice calls and different types of data calls. The system displays the **BCC Value** field when either the **ISDN-PRI** field or the **ISDN-BRI Trunks** field is set to y on the Optional Features screen.

  See the table on page 1419 for a description of BCC Values.

Table 126: Entries for the BCC Value area

Entry	Description
0	voice-grade data and voice
1	56-kbps data (mode 1)
2	64-kbps data (mode 2)
3	64-kbps data (mode 3)
4	64-kbps data (mode 0)
W	128-kbps to 1984-kbps data (wideband)

4. In the **BCIE** field, type the value that determines the creation of the ITC codepoint in the setup message.

   The **BCIE** field applies to ISDN trunks.

   - Type `ept` for endpoint.
   - Type `unr` for unrestricted.

     The system displays the **BCIE** field when the **ITC** field is set to both.

5. In the **CA-TSC** field, type the information for ISDN B-channel connections.

   See the table on page 1419 for a description of the entries for the **CA-TSC** field.

Table 127: Entries for the CA-TSC field

Entry	Description
as-needed	The CA-TSC is set up only when needed. This setting causes a slight delay. Avaya recommends this entry for most situations.
at-setup	The CA-TSC is automatically set up for every B-channel call whether or not it is needed.
none	No CA-TSC is set up. This setting permits tandeming of NCA-TSC setup requests.

6. In the **DCS/QSIG Intw** field, perform one of the following actions:
   - To enable CS/QSIG Voice Mail Interworking, type `y`.
   - To disable CS/QSIG Voice Mail Interworking, type `n`.

   The system displays the **DCS/QSIG Intw** field when the **Interworking with DCS** field is set to y on the Optional Features screen.
7. In the **FRL** field, type the Facility Restriction Level (FRL) that is associated with the preference.

   Valid values are the digits 0 through 7.

   0 is the least restrictive FRL, and 7 is the most restrictive FRL. To access the associated trunk-group, the FRL of the calling party must be greater than, or equal to, the FRL that you typed on this screen.

   Security alert:

   For system security reasons, Avaya recommends that you use the most restrictive FRL possible.
8. In the **Grp No** field, type the trunk group number that is associated with the preference.
   - Valid values are the digits 1 through 666 for DEFINITY R, CSI, and SI.
   - Valid values are the digits 1 through 2000 for the S8300D Server and IP-PNC.
9. In the **Hop Lmt** field, type the number of hops for each preference.

   A hop occurs when a call tandems through a media server or a system to another destination. You limit the number of hops to prevent circular hunting, which ties up trunk facilities without completing a call. The software blocks the number of hops that are equal to or greater than the number that you enter in the **Hop Lmt** field.

   See the table on page 1420 for the **Hop Lmt** field entries.

   Table 128: Entries for the Hop Lmt field

Entry	Description
blank	Indicates that the system does not apply a limit to the number of hops for this preference.
1 to 9	Limits the number of hops if you use the Tandem Hop capability. Valid values are the digits 1 to 9.
1 to 32	Limits the number of hops if you use the Transit capability. Valid values are the digits 1 to 32.

10. In the **Inserted Digits** field, type the digits that the software inserts for routing.

    Valid values are the digits 0 through 9. You can type a maximum of 36 digits.

    The software can send a maximum of 52 digits. This number includes the digits that you enter in the **Inserted Digits** field, plus the digits that the user dials. The software counts each special symbol as 2 digits.

See the table on page 1421 for the **Inserted Digits** field entries.

Table 129: Entries for the Inserted Digits field

Entry	Description
asterisk (*)	When an asterisk (*) is in the route pattern and the outgoing trunk is signaling type `mf`, the MFC tone for the “end-of-digits” is sent out to the central office (CO) in place of the asterisk (*).
pound sign (#)	When the pound sign (#) is in the route pattern and the outgoing trunk is signaling type `mf`, the MFC tone for the “end-of-digits” is sent out to the central office (CO) in place of the pound sign (#).
comma (,)	A comma (,) uses 2 places. A comma (,) creates a 1.5-second pause between the digits that are sent. Do not use a comma (,) as the first character in the string unless it is absolutely necessary. Misuse can result in some calls, such as Abbreviated Dialing or Last Number Dialed calls, not completing.
plus sign (+)	The plus sign (+) waits for dial tone up to the **Off Premises Tone Detection Timer**. The system then sends either digits or intercept tone, based on value in the **Out Pulse Without Tone** field on the Feature-Related System Parameters screen.
percent sign (%)	The percent sign (%) starts End-to-End Signaling.
exclamation point (!)	An exclamation point (!) waits for dial tone without timeout, and then sends dual-tone multifrequency (DTMF) digits.
ampersand (&)	An ampersand (&) waits for Automatic Number Identification (ANI). An ampersand (&) is used for Russian pulse trunks.
p	The associated trunk group must be of type “sip.” Type the single digit p for fully qualified E.164 numbers. The system translates the p to a plus sign (+). The system then places the plus sign (+) at the front of the digit string.
dollar sign ($)	If ($) sign is in the Inserted Digit String of a routing pattern, the MF Packet does not have ANI information. That is, use “1” S F11 format. If ($) is not in the Inserted Digit String of a routing pattern, the MF Packet shall have the “1” S Cs def xxxx F11 format.

11. In the **ITC** field, type the Information Transfer Capability (ITC) to identify the type of data transmission or traffic that this routing preference can carry.

    The ITC applies only to data calls BCC 1 through 4.

    If the **W** column of the **BCC** field is set to y, the **ITC** field must be set to either unre or both.

    See the table on page 1421 for **ITC** field entries.

Table 130: Entries for the ITC field

Entry	Description
both	Calls from restricted and unrestricted endpoints can access the route pattern.
rest	Calls from restricted endpoints can access the route pattern.
unre	Calls from unrestricted endpoints can access the route pattern.

12. In the **IXC** field, type the Inter-Exchange Carrier (IXC).

    The system uses this information for calls that the system routes through an IXC, and for the Call Detail Recording (CDR) feature.

    The system displays the **IXC** field when the **ISDN-PRI** field or **ISDN-BRI Trunks** field is set to y on the Optional Features screen.

    See the table on page 1422 for IXC field entries.

    Table 131: Entries for the IXC field

Entry	Description
Valid carrier code	Identifies the carrier for IXC calls.
user	Identifies a presubscribed carrier. Used when an IXC is not specified.
none	The **IXC** field must be none for non-ISDN trunk groups and for Bellcore NI-2 Operator Service Access. If you need to send an IXC code for a non-ISDN trunk group, type the IXC code in the **Inserted Digits** field.

13. In the **LAR** field, type the routing-preference for Look Ahead Routing (LAR).

    See the table on page 1422 for **LAR** field entries.

    Table 132: Entries for the LAR field

Entry	Description
next	Go to the next routing preference and attempt the call again.
rehu	Rehunt within the current routing-preference for another trunk to attempt the call again.
none	LAR is disbled for the preference.

14. In the **No.Del. Digits** field, type the total number of digits that you want the system to delete before the system sends the number out on the trunk.

    Valid values are the digits 0 through 28. You can also set the field to blank. To set the field to blank, press `Enter`.

    The software uses this information to modify the dialed number so that the system routes an AAR or ARS call over different trunk groups that terminate in media servers or systems with different dial plans. The software uses this information for the calls that use the following routing methods:

    - To or through a remote media server or switch
    - Over tie trunks to a private network server or switch
    - Over CO trunks to the serving CO

15. In the **No.Dgts Subaddress** field, type the number of dialed digits to send in the calling party subaddress information element (IE).

    You can change the **No. Dgts Subaddress** field if the **ISDN Feature Plus** field is set to y on the Optional Features screen.

Valid values are the digits 1 through 5. You can also set the field to blank. To set the field to blank, press `Enter`.

The software uses this information to route a call to a number where the media server deletes the dialed number and inserts the listed directory number (LDN). The LDN is then sent to the destination address, and the dialed extension is sent in the calling party subaddress IE. At the receiving end, the call terminates to the user who is indicated by the subaddress number instead of to the attendant.

16. In the **NPA** field, type the 3-digit Numbering Plan Area (NPA) for the terminating endpoint of the trunk group.

    The NPA is also known as the area code.

    Valid values are the digits 0 through 9. You can also set the field to blank. To set the to field blank, press `Enter`.

    For WATS trunks, the terminating NPA is the same as the home NPA unless the local exchange carrier (LEC) requires 10 digits for local NPA calls.

    Call your local telephone company to verify the NPA, if you need help.

    You do not need to enter an NPA for AAR.

17. In the **Numbering Format** field, type the information that specifies the format of the routing number that the system uses for the ISDN trunk groups for this preference.

    Note:

    To access the Bellcore NI-2 Operator Service Access, you must type `unk-unk` in the **Inserted Digits** field.

    The system displays the **Inserted Digits** field when the **ISDN-PRI or ISDN-BRI Trunks** field is set to y on the Optional Features screen.

    See the table on page 1423 for **Numbering Format** field entries.

Table 133: Entries for the Numbering Format field

Entry	Numbering Plan Identifier	Type of Numbering
blank	E.164(1)	1-MAX
natl-pub	E.164(1)	national(2)
intl-pub	E.164(1)	international(1)
locl-pub	E.164(1)	local/subscriber(4)
pub-unk	E.164(1)	unknown(0)
lev0-pvt	Private Numbering Plan - PNP(9)	local(4)
levl0-pvt (use this entry to allow Network Call Redirection / Transfer	-	-
lev1-pvt	Private Numbering Plan - PNP(9)	Regional Level 1(2)

Table continues…

Entry	Numbering Plan Identifier	Type of Numbering
lev2-pvt	Private Numbering Plan - PNP(9)	Regional Level 2(1)
unk-unk	unknown(0)	unknown(0)

The **Pattern Number** field is a display-only field that displays the route pattern number. The route pattern number is from 1 to 640.

18. In the **Prefix Mark** field, type the prefix mark information for ARS.

    Valid values are the digits 0 through 4. You can also set the field to blank. To set the field to blank, press `Enter`.

    This entry is not required for AAR.

    Prefix marks set the requirements for sending a prefix digit 1 to indicate a long distance call. Prefix marks apply to 7-digit Direct Distance Dialing (DDD) or 10-digit DDD public network calls. A prefix digit 1 is sent only when the **call type** field is a foreign number plan area (FNPA) or a home numbering plan area (HNPA) in the ARS Digit Analysis Table screen.

    For a WATS trunk, the prefix mark is the same as the local CO trunk.

    See the table on page 1424 for **Prefix Mark** field entries.

    Table 134: Entries for the Prefix Mark field

Entry	Description
0	• Suppress a user-dialed prefix digit 1 for 10-digit FNPA calls. • Leave a user-dialed prefix digit 1 for 7-digit HNPA calls. • Leave a prefix digit 1 on 10-digit calls that are neither FNPA nor HNPA calls. Do not use Prefix Mark 0 in those areas where all long distance calls must be dialed as 1 plus 10 digits. Check with your local network provider.
1	Send a 1 on all 10-digit calls, but not on 7-digit calls. Use Prefix Mark 1 for HNPA calls that require a 1 to indicate long distance calls.
2	Send a 1 on all 10-digit and 7-digit long distance calls. Prefix Mark 2 uses a Toll Table to define long distance codes.
3	Send a 1 on all long distance calls, and keep or insert the NPA so that all long distance calls are 10-digit calls. The system inserts the NPA when a user dials a prefix digit 1 plus 7 digits. Prefix Mark 3 uses a Toll Table to define long distance codes.
4	Always suppress a user-dialed Prefix digit 1. Use Prefix Mark 4, for example, when the system routes ISDN calls to a media server or a system that rejects calls with a prefix digit 1.
blank	For TIE trunks, leave this field blank.

19. In the **Service/Feature** field, type the IE in a call in this route pattern.

    Valid values are from 1 to 15 characters.

The **Service/Feature** field is required by Call-by-Call Service Selection, and Network Call Redirection and Transfer.

The system displays the **Service/Feature** field when the **ISDN-PRI** field or the **ISDN-BRI Trunks** field is set to y on the Optional Features screen.

See the table on page 1425 for **Service/Feature** field entries.

Table 135: Entries for the Service/Feature field

Entry	Description
accunet	-
i800	-
inwats	-
lds	-
mega800	-
megacom	-
multiquest	-
operator	-
oper-lds	Operator and lds
oper-meg	Operator and megacon
oper-sdn	Operator and sdn
outwats-bnd	-
sdn	Enter to allow Network Call Redirection/Transfer.
sub-operator	-
sub-op-lds	Suboperator and lds
sub-op-meg	Suboperator and megacom
sub-op-sdn	Suboperator and sdn
wats-max-bnd	-

20. In the **Toll List** field, type the number of the ARS Toll Table that is associated with the terminating NPA of the trunk group.

    You must complete this field if the **Prefix Mark** field is set to 2 or 3.

    Valid values are the digits 1 through 32. You can also set the field to blank. To set the field to blank, press `Enter`.

    This entry is not required for AAR.

21. In the **TSC** field, perform one of the following actions:

    - Type `y` if you want:
      - To allow Call-Associated TSCs, and to allow incoming Non-Call-Associated TSC requests to be tandemed out for each preference
      - Feature transparency on DCS+ calls and to use QSIG Call Completion

- Type `n` if you do not want:
  - To allow Call-Associated TSCs, and to allow incoming Non-Call-Associated TSC requests to be tandemed out for each preference
  - Feature transparency on DCS+ calls and to use QSIG Call Completion

Defining call types for World Class Routing

Procedure

1. Define operator-assisted calls
2. Define interexchange carrier calls

Defining operator-assisted calls for World Class Routing example

About this task

To define operator-assisted calls, the user first dials 9 to access ARS, then a 0, and the rest of the number, in this example, for an operator-assisted call to New Jersey.

Procedure

1. A user dials 9 0 908 956 1234.
2. The system:
   a. Ignores the ARS FAC, which is 9 in this example.
   b. Reviews the ARS Digit Analysis Table for 0.
   c. Determines that the user dialed more than 1 digit.
   d. Determines that the user dialed 11 digits.
   e. Rules out the dialed strings for 00, 01, and 011.
3. The system then routes the call as an operator-assisted call.

Defining interexchange carrier calls for World Class Routing example

Before you begin

1. Enter `display ars analysis n`, where *n* is the first number or numbers of the dialed string that you want to review.

   If you use an x in the **Dialed String** field, the system recognizes the x as a wildcard. The x represents any digit from 0 to 9. If you dial 1010, the next 3 digits always match the x wildcard in the dialed string.
2. Select **Enter** to exit the screen.

About this task

Interexchange carrier (IXC) numbers directly access your long distance carrier lines. IXC numbers begin with 1010. After 1010, IXC numbers include 3 digits, plus the number, including 0, 00, or 1 plus10 digits. These numbers are set up on your default translations.

Remember that the user first dials 9 in this example to access ARS, and then dials the rest of the number, in this example, for an IXC call to AT&T. 1010288 is the carrier access code for AT&T.

Procedure

1. A user dials 9 1010288, plus a public network number.
2. The system:
   a. Ignores the ARS FAC, which is 9 in this example.
   b. Reviews the ARS Digit Analysis Table for 1010.
   c. Analyzes the number.
3. The system then matches 288 with xxx, and sends the call over route pattern 5.

Using restricted area codes and prefixes for World Class Routing example

Before you begin

Enter `change ars analysis n`, where *n* is the first number or numbers of the dialed string that you want to review. After you review this information, press `Enter`.

About this task

Certain area code numbers are set aside in the North American Numbering Plan. For example, these numbers are 200, 300, 400, 500, 600, 700, 800, 877, 888, and 900. You must specifically deny calls made to area codes 200 through 900, except 800, 877, and 888.

If you do not want to incur charges, you can also deny access to the 976 prefix. The 976 prefix is set aside in each area code for pay-per-call services. You can block 976 or any other prefix in all Numbering Plan Areas (NPAs) with a single entry in the digit analysis table.

You can 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.

In this example, that begins with 120, where the call is permitted. The 120 translation handles all dialed strings from 1201 through 1209.

Procedure

1. A user dials 9 120, plus 8 digits, the first of which is not 0.
2. The system:
   a. Ignores the ARS FAC, which is 9 in this example.
   b. Reviews the ARS Digit Analysis Table for the numbers 120.
   c. Analyzes the number.
   d. Determines that the call is long distance.
   e. Sends the call over Route Pattern 4.

   • Follow the routing for the call, in this example, that begins with the restricted area code 200:
3. A user dials 9 1200, plus 7 digits.

4. The system:
    a. Ignores the ARS FAC, which is 9 in this example.
    b. Reviews the ARS Digit Analysis Table for the numbers 1200.
    c. Analyzes the number.
    d. Determines that the Call Type is deny. The call does not go through.

Using wildcards for World Class Routing example

About this task

You can use wildcards to help control calls to certain numbers. When you use the wildcard x in the **Dialed String** field, the system recognizes x as any digit from 0 to 9.

For this example, use wildcards to restrict users from making calls to a 555 information operator where you might incur charges. The wildcards in this example represent any area code that the user might dial.

Procedure

1. Enter `change ars analysis n`, where *n* is the first number or numbers of the dialed string that you want to review.

   In this example, the number is 1. Press `Enter`.
2. Click **Next** if necessary until you see a blank field.
3. In the Dialed String column, type `1xxx555`.

   In this example, the:

   - indicates a long distance call.
   - xxx indicates any three numbers, or area code, from 000 to 999.
   - indicates the extension prefix that you want to restrict.
4. In the **Total Min** and the **Total Max** columns, type `11`.

   In this example, the number 11 in both columns indicates that total length of the dialed number must be 11 digits.
5. In the **Route Pattern** column, type `deny`.
6. In the **Call Type** column, type `fnhp`.
7. Select **Enter** to save your changes.

Defining local information calls for World Class Routing example

About this task

You might want users to access local information. In this example, allow users to dial extension 411 to access local information.

Procedure

1. Enter `change ars analysis n`, where *n* is the first number or numbers of the dialed string that you want to review.

   In this example, the number is 4. Press `Enter`.

2. Click **Next** if necessary until you see a blank field.
3. In the **Dialed String** column, type the string of numbers that you want to change.

   In this example, type `411`.

4. In the **Total Min** and the **Total Max** columns, type the minimum number of digits, and the maximum number of digits, that you want the system to analyze.

   In this example, the number 3 in both columns indicates that total length of the dialed number must be 3 digits.

5. In the **Route Pattern** column, type a routing pattern number.

   In this example, type the number `1`.

6. In the **Call Type** column, type `svcl`.

   The call type svcl indicates a service call.

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

Modifying call routing

Procedure

1. Add a new area code.
2. Add a new prefix.
3. Use ARS to restrict outgoing calls.

   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 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 for World Class Routing example

Before you begin

1. Enter `list ars route-chosen`, the number **1**, the existing area code, and any 7-digit telephone number.
2. For this example, type `list ars route-chosen 14152223333`. Press Enter.
3. Remember the **Total Min**, **Total Max**, **Route Pattern**, and **Call Type** values on this screen.

   In this example, the **Total Min** is 11, the **Total Max** is 11, the **Route Pattern** is 30, and the **Call Type** is fnpa.

4. Select **Enter** to exit the screen.

About this task

Sometimes, area codes within a region might change. In this example, area code 415 has split into two area codes, 415 and 650. Add a new nonlocal area code, 650, to have the same values as the existing nonlocal area code on your system, 415.

In this example, add a new area code 650 that has the same values as area code 415.

Procedure

1. Enter `change ars analysis n`, where *n* is the first number or numbers of the dialed string that you want to review. In this example, the number is 1650.

   The system displays the ARS Digit Analysis Table screen for dialed strings that begin with the numbers 1650

2. Click **Next** if necessary until you see a blank field.

   If the dialed string is already defined in your system, the system displays the cursor in the appropriate **Dialed String** column where you can make changes.

3. In the Dialed String column, type `1650`.

4. In the **Total Min** and the **Total Max** columns, type the minimum and maximum values.

   For this example, the minimum and maximum values are 11.

5. In the **Route Pattern** column, type the route pattern.

   For this example, the route pattern is 30.

6. In the **Call Type** column, type the call type.

   For this example, the route pattern is fnpa.

7. In the **Node Num** column, type the node number.

   For this example, the node number is left blank.

8. Select **Enter** to save your changes.

Adding a new prefix for World Class Routing example

About this task

To add a new prefix, follow the same procedure as you use to add a new area code. The one exception is to use a shorter dial string (such as **2223333**, where **222** is the old prefix,) and a dial type of hnpa.

If you do not need to use the number 1 for area code calls, omit the 1 in Step 1, Step 4, and Step 6 in the previous procedure. Also, type `10` instead of `11` in the **Total Min** and the **Total Max** fields in Step 7.

To see if the new area code or prefix number is set up as a toll call, type **display toll n**, where **n** is the prefix that you want to review. Some users might be disallowed to dial toll call numbers.

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. In the US, you can restrict access to 900 and 976 pay-per-call numbers.

In this example, Colombia is used as the country to restrict. The country code for Colombia is 57.

To prevent callers from placing calls to countries that you want to restrict:

Procedure

1. Enter `change ars analysis 011n`, where *011* is the international access code and *n* is the country code of the restricted country.

   In this example the country code of the restricted country is 57.

2. Click **Next** if necessary until you see a blank field.

   If the dialed string is already defined in your system, the system displays the cursor in the appropriate **Dialed String** column. Skip to Step 5 to deny calls to this dialed string.

3. In the Dialed String column, type `011xx`, where xx is the country code of the restricted country.

   In this example, type `01157`.

4. In the Total Min and the Total Max columns, type the minimum number of digits, and the maximum number of digits, that you want the system to analyze.

   In this example, type `10` in the **Total Min** column, and `23` in the **Total Min** column. The system uses this digit analysis entry if the dialed number:

   - Begins with 01157.
   - Contains at lease 10 digits.
   - Contains no more than 23 digits.

5. In the **Route Pattern** column, type an appropriate route pattern.

   In this example, type `deny` to prevent users to complete calls to this dialed string.

6. In the **Call Type** column, type the category of calls that this dialed string represents.

   In this example, type `intl` to indicate this dialed string represents an international call.

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

ARS partition definition

You can use ARS partitioning to provide different call routing for a group of users, or for specific telephones.

If you used partitioning on a prior release of Communication Manager and you want to continue to use partitioning, read this section carefully. In Communication Manager Release 2.0, partition

groups are defined on the Partition Route Table. Partition groups are no longer defined on the Digit Analysis Table.

Preparing to define ARS partitions

Procedure

1. Enter `display system-parameters customer-options`.
2. Ensure that the **Tenant Partitioning** field is set to y.

   If this field is set to n, go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to ARS partitions, or to open a service request.
3. Ensure that the **Time of Day Routing** field is set to n.

   If this field is set to y, go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to ARS partitions, or to open a service request.

Setting up partition groups example

About this task

In this example, your company provides your employees to make local, long distance, and emergency calls. However, you have a telephone in the lobby for visitors. You want to allow visitors to make only local, toll-free, and emergency calls from this telephone.

To restrict the telephone in the lobby, modify the routing for a partition group to enable only specific calls, such as US-based toll-free 1-800 calls. Then assign this partition group to the telephone. In this example, the partition group for the telephone in the lobby is partition group 2.

Procedure

1. Enter `list ars route-chosen 1800n`, where *n* is any 7-digit telephone number to create an example of the dialed string.

   In this example, type `18002221000`.
2. Note the route pattern for the selected dialed string.

   In this example, the route pattern for 1800 is p1. p1 indicates that the system uses the Partition Routing Table to determine what route pattern to use for each partition.

   If the system displays a number in the Route Pattern column without the letter p, all partitions use the same route pattern. You need to use the Partition Routing Table only if you want to use different route patterns for different partition groups.
3. Select **Enter** to exit the screen.
4. Enter `change partition-route-table index n`, where *n* is the route index number.

   In this example, the route index number is 1.
5. In the **PGN 2** column that corresponds to **Route Index 1**, type the same number as in the **PGN 1** column.

In this example, type `30`.

This entry tells the system to use route pattern 30 for partition group 2, and allow partition group 2 members to make calls to 1-800 numbers.

6. Select **Enter** to save your changes.

Assigning a telephone to a partition group

About this task

Assigning a telephone extension to a partition group is a two-step process. First, assign the partition group to a COR. Then assign that COR to the extension.

Procedure

1. Enter `list cor`.
2. Choose a COR that is not used.

   In this example, use COR number 3.
3. After you review this information, press `Enter` to exit the screen.
4. Enter `change cor` *x*, where *x* is the COR number that you just chose.

   In this example, the COR number is 3.
5. In the **COR Description** field, type a name for this COR.

   In this example, the COR name is lobby, named for the telephone in the lobby.
6. In the **Partitioned Group Number** field, type the number of the partition group.

   In this example, the partition group number is 2.
7. Select **Enter** to save your changes.
8. Enter `change station` *n*, where *n* is the extension.
9. In the **COR** field, type the number of the COR.

   In this example, the COR number is 3.
10. Select **Enter** to save your changes.

Time of Day Routing administration

You can use Time of Day Routing to redirect calls to coverage paths according to the time of the day and the day of the week. You must define the coverage paths that 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 the day of the week that 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 that the system uses for call forwarding to external numbers.

Preparing to administer Time of Day Routing example

About this task

AAR or ARS must be administered on the system before you can use Time of Day Routing.

Procedure

On the Optional Features screen:

- For AAR, ensure that either the **Private Networking** field or the **Uniform Dialing Plan** field is set to y. If either of the fields is set to n, go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Time of Day Routing, or to open a service request.
- For ARS, ensure that the **ARS** field is set to y, and the **Time of Day Routing** field is set to y. If both these fields are not set to y, your system does not support the Time of Day Routing feature. Go to the Avaya Support website at http://support.avaya.com for current documentation and knowledge articles related to administering Time of Day Routing, or to open a service request.

  To view the Optional Features screen, enter `display system-parameters customer-options`.

Displaying the Time of Day Routing plan example

Procedure

1. Enter `display time-of-day n`, where *n* is the number of the routing plan.

   In this example, the number of the routing plan is 1.

   Note the routing plan that is currently in effect. In this example, this plan is for employees who can make only local calls.

   In this example, two partition group numbers (PGN) control Time-of-Day routing:

   - PGN 1 begins 1 minute after midnight (00:01) every work day of the week until 8:00 a.m.
   - PGN 2 begins at 8:00 a.m. every work day of the week until 12:00 p.m.
   - PGN 1 begins at 12:00 p.m. every work day of the week until 1:00 p.m. (13:00).
   - PGN 2 begins at 1:00 p.m. (13:00) every work day of the week until 5:00 p.m. (17:00).
   - PGN 2 begins at 5:00 p.m. (17:00) every work day of the week until 12:00 a.m.
   - PGN 1 is also used all day Saturday and Sunday.
2. After you review this information, click **Cancel**.

Creating a Time of Day Routing plan example

Procedure

1. Enter `change time-of-day n`, where *n* is the number of the routing plan.

   In this example, the number of the routing plan is 2.

2. In the first **PGN #** column, type `1` in each field.

   In this example, PGN 1 is the partition group that the system uses for after hours and the lunch hour.

3. In the remaining **PGN #** columns, type `3` in all fields.

   In our example, PGN 3 is the partition group that the system uses to route long distance calls during business hours.

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

5. Now assign your new Time of Day Routing Plan 2 to the COR that is assigned to your executives.

   In this example, the following conditions are true:

   - 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.

   When Jim comes into work on Monday morning at 8:30 and 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 the COR for Jim.

   Because Jim has been assigned COR 2 with Time of Day Plan Number 1, the system uses Time of Day Routing Plan 1 to route the call.

   According to the Time of Day Routing Plan 1, the system routes calls that are made between 8:00 a.m. and 11:59 a.m. according to the route pattern that is set up in the PGN 1 column.

   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.

Interactions for World Class Routing

This section provides information about how the World Class Routing feature interact with other features on the system. Use this information to ensure that you receive the maximum benefits World Class Routing in any feature configuration:

Bridged Call Appearance

If a Bridged Call Appearance is used for an Automatic Alternate Routing (AAR) or an Automatic Route Selection (ARS) call, the system uses the partition group number (PGN) of the bridged extension instead of the PGN of the caller.

Call Forwarding

The system uses the PGN of the COR of the forwarding party to select the table to look up the route pattern.

Distributed Communications System (DCS)

When the system routes a call over DCS, the far-end switch uses the PGN of the incoming trunk to route the call.

Remote Access

When a remote-access user dials a barrier code or an authorization code plus an ARS Feature Access Code (FAC), the COR of the barrier code or authorization code determines the PGN.

Straightforward Outward Completion and Through Dialing

If the attendant assists or extends a call and dials an ARS FAC, the COR of the attendant determines the PGN if the individual extension is assigned. If the individual extension is unassigned, the COR that is set on the console parameter determines the PGN.

ARS/AAR Dialing Without FAC interactions

The following features require entries in the **ARS/AAR Internal Call Prefix** and **Total Length** fields on the Dial Plan Parameters screen, if you intend to dial a shortcut ARS/AAR number after the applicable FAC or button push:

- Add/remove skill
- Attendant activation of call forwarding
- Call forwarding activation
- CDR reports
- Changeable COR through FAC
- Coverage Message Retrieval
- EC500 feature activation
- Extended call forwarding
- Leave Word Calling activation/cancellation
- Station Security Code Change
- TTI
- User/Group Controlled Restriction
- Whisper Paging

Chapter 190: 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.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments	Describes the implementation instructions while deploying Communication Manager on a software-only environment and Amazon Web Service, Microsoft Azure, and Google Cloud Platform.	Implementation Engineers, Support Personnel, Solution Architects

Table continues…

Title	Description	Audience
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 specific customers request 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, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Select Release**, select the appropriate release number.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
9. Press **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.

5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Choose Release**, select the required release number.
9. 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.
10. Press **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation 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 keywords.

  To filter by product, click **Filters** and select a product.
- Search for documents.

  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 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 the 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 in to the website. The available functionality depends on your role.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click **>** to search for the course.

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
20980W	What's New with Avaya Aura®
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager Release 10.1
61451V	Administering Avaya Aura® Communication Manager Release 10.1

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 keyword or keywords 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 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 https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.

   The system displays the Avaya Support page.
5. Click **Support by Product** > **Product-specific Support**.
6. In **Enter Product Name**, enter the product, and press `Enter`.
7. Select the product from the list, and select a release.
8. Click the **Technical Solutions** tab to see articles.
9. Select **Related Information**.

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) 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 and log in.
2. On the top of the page, in **Search Product**, type the product name.

   The Avaya Support website displays the product name.
3. Select the required product name.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. On the product page, click **Product Documents**.
6. In the Latest Support, Service and Product Correction Notices section, click **View All Notices**.
7. 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 service packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to https://support.avaya.com and search for “Guide to Managing Your Avaya Access Profile for Customers and Partners”.

   Under the Search Results section, click Guide to Managing Your Avaya Access Profile for Customers and Partners.

2. Set up e-notifications.

   For detailed information, see the **Subscribe to E-Notifications** procedure.

Index

Special Characters

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W