Administering Network Connectivity on Avaya Aura® Communication Manager

Release 10.2.x
Issue 3
December 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 book provides background information about the network components of Avaya Aura® Communication Manager.

You can refer to the book when you:

- Connect Avaya phones to various networks.
- Configure Avaya phones.
- Configure Port Networks (PN).
- Administer converged network components, such as Avaya Aura® Media Server, gateways, trunks, fax, modem, TTY, and clear-channel calls.

This document is intended for anyone who wants to gain a high-level understanding of the product features, functionality, capacities, and limitations within the context of solutions and verified reference configurations.

- Technical support representatives
- Authorized Business Partner

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

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.

Change history

Issue	Date	Summary of changes
3	December 2024	Deleted the following section: • Network Region Wizard
2	July 2024	Updated the section: Branch office networks
1	December 2023	Release 10.2

Chapter 2: Networking Overview

Network terminology

The Communication Manager network can contain multiple servers and equipment, including data-networking devices that servers control. Such equipment might be geographically dispersed across many sites. Each site might segregate equipment into distinct logical groupings of endpoints, including stations, trunks, and gateways, referred to as network regions. A single server system has one or more network regions. If one server is inadequate for controlling the equipment, multiple systems can be networked together. One or more network regions make a site, and one or more sites make a system, which in turn is a component of a network.

Types of networks:

- Nondedicated network: Businesses have a corporate network, such as a LAN or a WAN. Over this corporate network, businesses distribute emails and data files, run applications, access the Internet, and exchange fax and modem calls.

  This type of network and the traffic that it bears is a nondedicated network. The network is a heterogeneous mix of data types.
- Converged network: A nondedicated network that carries digitized voice signals with other data types is a converged network. The converged network is a confluence of voice and nonvoice data.
- Dedicated network: Network segments that carry telephony traffic are dedicated networks because the network segments carry only telephony-related information.
- IP network: A digital network carries telephony and non telephony data in a packet-switched environment, such as TCP/IP, instead of a circuit-switched environment, such as TDM. The digital network is an IP network.

Digital telephone calls

A digital telephone call consists of voice data and call-signaling messages. Some transmission protocols require transmission of signaling data over a separate network, virtual path, or channel from the voice data. Data that is transmitted between switches during a telephone call includes:

- Voice data that contains digitized voice signals
- Call-signaling data with control messages

Network regions

A network region is a group of IP endpoints that share common characteristics and common resources. Every IP endpoint on the Communication Manager system belongs to a network region. You can differentiate between the network regions either by the resources assigned or the geographical location or both.

You can create different network regions when a group of endpoints:

- Require a different codec set based on bandwidth allocation or a different encryption algorithm than another group.
- Gain access to specific PROCR, gateways, or other IP resources.
- Require a different UDP port range or QoS parameters than another group.
- Report to a different VoIP Monitoring Manager server than another group.
- Require a different codec set based on bandwidth requirement or encryption algorithm for calls within the group than calls between separate endpoint groups.

The concept of locations is also similar to network regions. Use the location parameter to:

- Identify distinct geographic locations, primarily for call routing purposes.
- Ensure that calls pass through proper trunks based on the origin and destination of each call.

Communication Manager supports 2000 locations and network regions. You can now configure network regions as core network regions and stub network regions. You can configure network regions from 1 to 250 as core network regions or stub network regions. Network regions 251 to 2000 are stub network regions. A core network region is the traditional network region and can have multiple direct links with other network regions. For a diagrammatic representation of core network regions, see Figure 1: Core network regions on page 10. The solid lines in the diagram indicate a direct communication path between two core network regions. The dotted lines indicate an indirect logical communication path between two core network regions.

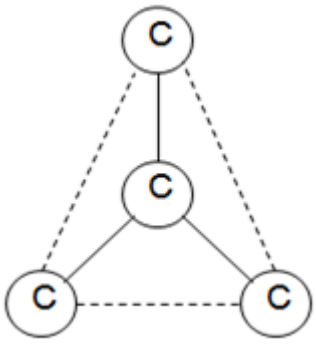


Figure 1: Core network regions

A stub network region must have a single defined pathway to only one core network region. For a diagrammatic representation of core network regions and stub network regions, see Figure 2: Core and stub network regions on page 11.

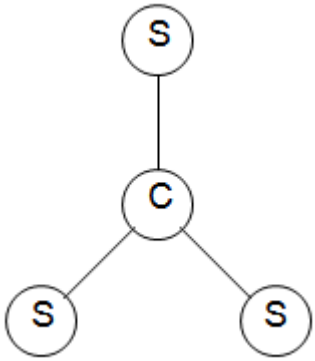


Figure 2: Core and stub network regions

Stub network regions communicate with other network regions using the defined communication pathways of the core network regions. For example, a scenario where stub network region 251 directly communicates with core network region 1. If stub network region 251 wants to send data to core network region 3, then stub network region 251 first sends data to core network region 1. From core network region 1, Communication Manager uses the predefined communication pathway of core network region 1 to reach core network region 3. For a diagrammatic representation of the communication pathway, see Figure 3: Communication Pathway from a stub network region to a core network region on page 11.

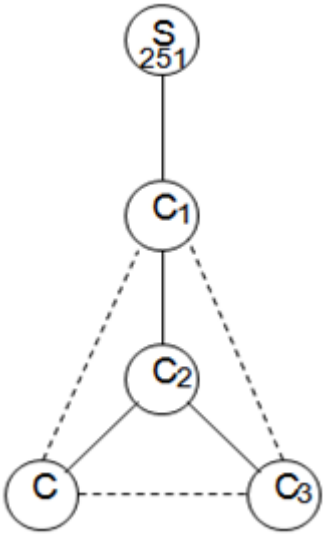


Figure 3: Communication Pathway from a stub network region to a core network region

The benefit of having a stub network region is that you do not have to configure multiple communication pathways to different network regions. When you add a stub network region, administer the communication path only to the core network region to which the stub network region connects.

Features affected by the increase in locations and network regions

The increase in the number of network regions and locations can affect the following features:

- Dial Plan Transparency (DPT): The DPT feature can work in a stub network region only with endpoints. Stub network regions use the media processing resources of the core network regions that the stub network regions connect to. Administer the DPT feature in a core network region that is directly linked with other stub network regions. Only then can the endpoints in the stub network regions connect to endpoints in other network regions.
- Inter-gateway Alternate Routing (IGAR): Any stub network region from 1 to 250 can use IGAR if the stub network region contains a branch gateway or a port network. IGAR is unavailable for stub network regions from 251 to 2000.
- Emergency Calling: When an endpoint in a stub network region dials an emergency number, Communication Manager analyzes the dialed number. Communication Manager then uses the ARS location table to route the call to the destination. The call is routed using a predefined route pattern.

Interswitch trunk connections

You can use the connected switches within an enterprise to communicate easily, regardless of the location or the communication server that the switches use. Interswitch connections also provide shared communications resources, such as messaging and call center services.

Switches communicate with each other over trunk connections. Different types of trunks provide different sets of services. Commonly used trunk types are:

- Central Office (CO) trunks that provide connections to the public telephone network through a central office.
- H.323 trunks that send voice and fax data over the Internet to other systems with H.323 trunk capability.
- H.323 trunks that support DCS+ and QSIG signaling.
- Tie trunks that connect switches in a private network.
- SIP trunk equipped with SIP signaling

For more information about the trunk types, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Branch office networks

The G4xx Media Gateways offer interfaces for digital and analog stations, trunks, and various media services, such as facilitating 6-party conferences and announcements. Until Avaya Aura® Release 10.1, G4xx Media Gateways were installable solely in branch offices connected to a common network with other branches and the headquarter sites.

Since the Avaya Aura® Release 10.1, the G4xx Media Gateway supports a new network topology (Edge Friendly) where branch offices are on separate networks, interconnected through the Internet or through SD-WAN.

With the Release 10.2, the survivable components, Survivable Remote Server (LSP), and Branch Session Manager (BSM), can also deploy in the Edge Friendly topology. The Edge Friendly configuration facilitates integration between on-premises gateways and survivable servers with a core Communication Manager hosted in the Cloud.

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a loop avoidance protocol. If your network does not have loops, you do not need STP. However, you must always enable STP. If you do not enable STP, all traffic stops on the network with a loop or with the wrong cable plugged into wrong ports.

However, STP is slow to converge after a network failure and provide a new port into the network. By default, the speed is ~50 seconds.

A modified version of STP is the Rapid Spanning Tree protocol. Rapid Spanning Tree converges faster than STP and enables new ports faster than the older protocol. As the Rapid Spanning Tree protocol works with all Avaya equipment, use the Rapid Spanning Tree protocol.

Inter-Gateway Alternate Routing

With Inter-Gateway Alternate Routing (IGAR), Communication Manager can use the PSTN instead of the IP-WAN for bearer connections. This feature is beneficial 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 extends this support to SIP endpoints.

IGAR requests PSTN to provide bearer connections in any of the following conditions:

- Reaching the number of calls or bandwidth allocated through Call Admission Control-Bandwidth Limits (CAC-BL).
- Facing VoIP RTP resource exhaustion in a port network or media gateway.
- Encountering the codec set between a pair of network regions set to `pstn`.
- Finding forced redirection configured between a pair of network regions.

IGAR provides enhanced Quality of Service (QoS) to large, distributed single-server configurations. IGAR is intended 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 inter-NR 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 another NR. The Trunk IGC is independent of the call. Therefore, Communication Manager can originate the IGC from the NR of the calling party to the NR of the called party, or vice versa. Some users use Facility Restriction Levels or Toll Restriction to determine who gets access to IGAR resources during a WAN outage. For these users, the calling user is considered the originator of the Trunk IGC for authorization and routing. For outgoing trunk groups administered to send the Calling Number, the IGAR Extension in the originating NR is used to create this number using the appropriate administration.

A few 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. If no coverage path is assigned, the calling party hears a busy tone.
- If the unreachable endpoint is 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. The system tries to route the call to another agent using the administered group type, such as Circular distribution and Percent Allocation Distribution.

Dial Plan Transparency

Dial Plan Transparency (DPT) preserves the dial plan when a gateway registers with a Survivable Remote server or when a port network registers with a Survivable Core server. Port network registers with a Survivable Core server due to the loss of contact with the primary controller. DPT

establishes a trunk call and reroutes the call over the PSTN to connect endpoints that can no longer connect over the corporate IP network.

You need not activate DPT in the license file. DPT is a standard feature in Communication Manager Release 4.0 and later. DPT is similar to IGAR as both provide alternate call routing when normal connections are unavailable. A major difference is that DPT routes calls between endpoints that two independent servers control. IGAR routes calls between endpoints that a single server controls. The DPT and IGAR features are independent of each other, but you can activate both simultaneously.

Limitations of DPT:

- DPT only handles IP network connectivity failures between network regions.
- DPT calls are trunk calls. Therefore, Communication Manager does not support many station features.
- For Release 4.0, DPT applies only to endpoints that are dialed directly. DPT cannot route redirected calls or calls to groups.
- DPT cannot reroute calls involving a SIP endpoint that has lost registration with the Session Manager.
- DPT works only when failover strategies for gateways and port networks, and alternate gatekeeper lists for IP stations are consistent.

For information about administering DPT, see Administering DPT on page 100.

Network quality management

A successful Voice over Internet Protocol (VoIP) implementation involves quality of service (QoS) management that is affected by three major factors:

- Delay: Significant end-to-end delay can cause echo and talker overlap.
- Packet loss: During peak network loads and periods of congestion, voice data packets might drop.
- Jitter (Delay variability): Data packets arrive at their destination at irregular intervals because of variable transmission delay over the network.

For more information about these QoS factors and network quality management, see:

- Chapter 6: Voice and Network quality administration on page 73.
- *Avaya Aura® Core Solution Description* .

VoIP transmission hardware

The following circuit packs are essential in an Avaya telecommunications network:

- Avaya Aura® Media Server

  Provide high-capacity VoIP audio access to the switch for local stations and outside trunks.

  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.

- Branch gateways

  Provide:

  - Extension of Communication Manager telephony features to branch offices when controlled by a remote server.
  - Standalone telephony systems when controlled by an embedded S8300E.
  - Survivable Remote server backup for a remote server.

  The branch gateways include the G430 Branch Gateway, G450 Branch Gateway, and IG550.

  Note:

  S8300E supports G430 Branch Gateway and G450 Branch Gateway.

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

Processor Ethernet

Processor Ethernet (PE) provides connectivity to IP endpoints, gateways, and adjuncts. The PE interface is a logical connection in the Communication Manager software that uses a port on the NIC in the server. The NIC is the s-called native NIC. PE uses the PROCR IP-interface type. You do not need additional hardware to implement PE.

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

For more information about how to configure the server, see *Administering Avaya Aura® Communication Manager*.

A Survivable Remote server or a Survivable Core server enables the Processor Ethernet interface automatically. Using the PE interface, you can register H.248 gateways and H.323 endpoints on the Survivable Remote server. You must set the H.248 and the H.323 fields on the IP Interface Procr screen to the default value `yes`.

Branch Gateway and H.323 endpoint registration on the Survivable Core server is possible. Administer the **Enable PE for H.248 Gateways** and **Enable PE for H.323 Endpoints** fields

on the Survivable Processor screen of the main server. The IP Interface Procr screen of the Survivable Core server displays the values that you administered for the H.248 and H.323 fields.

Important:

Both the Survivable Core server and the Survivable Remote server require the PE interface to register to the main server. Do not disable the PE interface on either server.

Support for Processor Ethernet on a Survivable Core server

The capabilities of survivable core servers are enhanced to support the connection of IP devices to the Processor Ethernet (PE) interface.

A survivable core server can use the PE interface to support IP devices, such as Branch Gateway, H.323 Gateways, IP Adjuncts, IP telephones, IP trunks, and SIP trunks. The survivable core server can provide the equivalent benefit of a survivable remote server. The survivable core server can be duplicated, providing more redundancy to the survivability of the system.

For PE on duplex servers to work, assign the PE interface to the PE Active server IP address and not the server unique address. The NIC assigned to the Processor Ethernet interface must be on a LAN connected to the main server.

- If the survivable remote server or the survivable core server registers to PE on the main server, PE must have IP connectivity to the LAN. The LAN must be assigned to the NIC used for PE on the survivable core server.

Firmware for optimal performance

Processor Ethernet on duplex servers works effectively only when the branch gateways and IP telephones are on the current release of the firmware.

Use the following IP telephone models to ensure optimal system performance when you use Processor Ethernet on duplex servers:

- J129, J139, J159, J179, and J189.
- 9608G, 9611G, 9621G, and 9641G.
- 1608, and 1616.
- 9610, 9620, 9630, 9640, and 9650 telephones with firmware 3.0 or later. Any later 96xx and 96x1 models that support Time to Service (TTS) work optimally.
- 4601+, 4602SW+, 4610SW, 4620SW, 4621SW, 4622SW, and 4625SW Broadcom telephones with firmware R 2.9 SP1 or later. 46xx telephones are supported if the 46xx telephones are not in the same subnetwork as the servers.

All other IP telephone models must reregister if a server interchange occurs. The 46xx telephones reregister if the telephones are in the same subnetwork as the servers.

To ensure that you have the most current versions of firmware, go to the Avaya Support website at http://support.avaya.com. Click **Downloads** and select the product.

LAN security

Customers do not want users to access the switch by using the INADS line. When users use the INADS line, users continue to PROCR and then gain access to a customer LAN. However, the Avaya architecture prevents users from accessing the customer LAN.Figure 4: Security-related system architecture on page 18 shows a high-level switch schematic with a TN799 (PROCR).

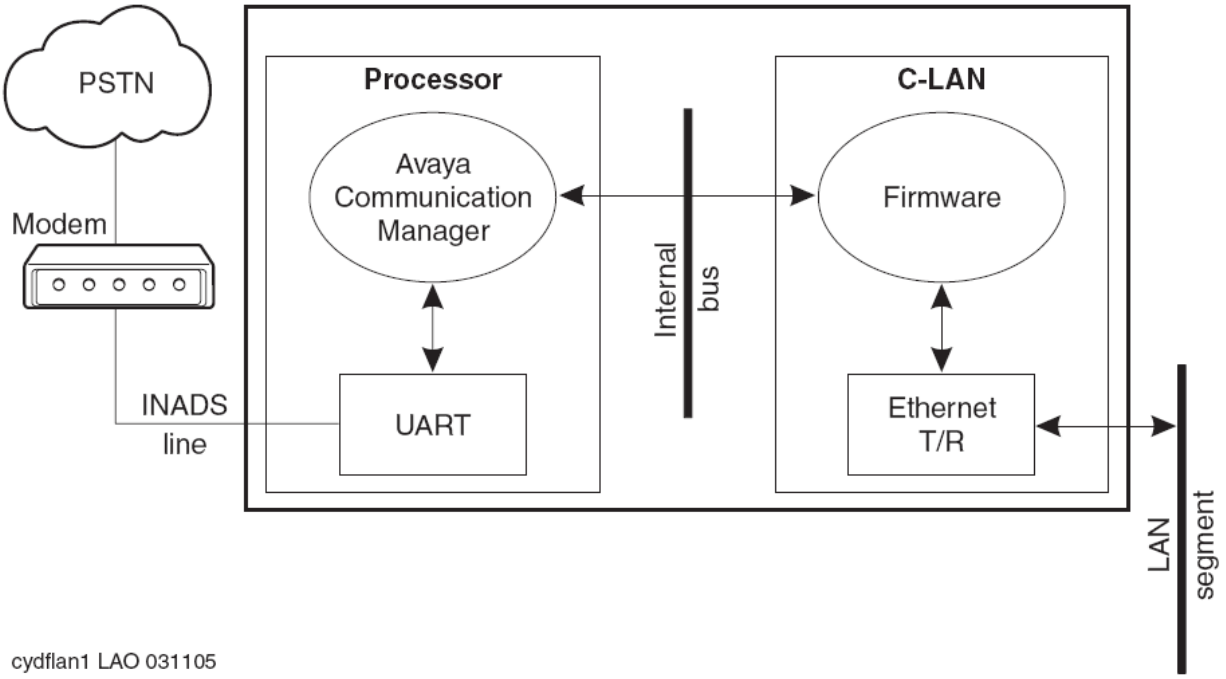


Figure 4: Security-related system architecture

Logging in through the INADS line, customers can access software. Software communicates with firmware over an internal bus through a limited message set. The two main reasons why a user cannot go to the customer LAN through the INADS line are:

- A user logging into software cannot get direct access to the PROCR firmware.

  The user can only enter SAT commands that request PROCR information or configure PROCR connections.

- Communication Manager disables the PROCR application TFTP and cannot enable the application.

  TELNET only interconnects PROCR Ethernet clients to the system management application on the switch. FTP exists only as a server and is used only for firmware downloads. FTP cannot connect to the client network.

Connection Preservation

Communication Manager supports Connection Preservation and Call Preservation for handling SIP calls. Any SIP telephone connected to Communication Manager through a server that enables SIP can use this feature. SIP Connection Preservation and Call Preservation are always active.

Call Preservation and Connection Preservation during LAN failure

When near-end failure is detected, the SIP signaling group state changes to the Out-of-service state. The SIP trunk in the trunk group is in a deactivated state and cannot be used either for incoming or outgoing calls. Stable or active calls on the SIP trunk are not dropped and are kept in the In-service/active state. When the active connection is dropped, SIP trunk changes to the Out-of-service state. When far-end failure is detected, the SIP signaling group state changes to the Far-end-bypass state. Stable or active calls are not dropped, and the SIP trunk changes to the pending-busyout state. When the active connection is dropped, the SIP trunk status changes to the Out-Of-Serivce/FarEnd-idle state.

Call Preservation and Connection Preservation when LAN connectivity is revived

When the near-end failure ends, the SIP signaling group state changes to the In-service/active state. Stable or active calls on the SIP-trunk are kept in the In-service/active state. When the far-end failure ends, the SIP signaling group state changes to the In-service/active state. The state of Stable or active calls on the SIP trunk changes from pending-busyout to the In-service/active state.

The Connection Preservation mechanism also works with DCP and H.323 telephones.

Session refresh handling

When SIP session refresh handling fails, the SIP call is set to Connection Preservation. A net safety timer keeps the call active for 2 hours. After 2 hours, the call drops unless the user ends the call before that time.

Connection Preserving Migration

The Connection Preserving Migration (CPM) feature preserves bearer connections while Branch Gateway migrates from one Communication Manager server to another because of network failure or server failure. Users on connection preserved calls cannot use features such as Hold, Conference, or Transfer.

CPM does the following:

- Preserves the audio voice paths.
- Extends the period for recovery operations.
- Continues to function during the complementary recovery strategies of Avaya.

H.248 and H.323 link recovery

The H.248 link connects a Communication Manager server and a gateway. The H.323 link connects ties a gateway and an H.323-compliant IP endpoint. Link recovery is an automated method that the gateway uses to reacquire a lost link. The link might be lost from either a primary

call controller or a Survivable Remote server. The H.248 link and the H.323 link provide the signaling protocol for:

- Call setup
- Call control during the call
- Call tear-down

When the link is out of service, link recovery preserves calls and attempts to reestablish the original link. If the gateway or the endpoint cannot reconnect to the original server or gateway, then link recovery automatically attempts to connect with alternate TN799DP (PROCR) circuit packs. Link recovery only connects with circuit packs that are within the configuration of the original server or the Survivable Remote server.

Auto fallback to the primary server

The auto fallback to primary controller feature returns a fragmented network to the primary server automatically. Fragmented networks have a number of branch gateways that one or more Survivable Remote servers service. This feature applies to all branch gateways. You can complete the distributed telephony switch network by automatically migrating the gateways back to the primary server.

Survivable Remote servers

Survivable remote servers can function as survivable call processing servers for remote or branch customer locations. Survivable remote servers have a complete set of Communication Manager features. With the license file, survivable remote servers function as survivable call processors.

If the link between the remote branch gateways and the primary controller breaks, the telephones and the gateways register with the survivable remote server. Survivable remote servers provide a backup service to the registered devices and control these devices in a license-error mode.

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

Note:

The Survivable Remote Server is also known as Local Survivable Processor (LSP). From Communication Manager Release 10.2, Local Survivable Processor supports the Edge Friendly network topology.

Survivable core servers

Survivable core servers provide survivability to port networks by putting backup servers in various locations in the customer network. The backup servers service port networks when:

- The Simplex server fails.
- The Duplex server pair fails.
- connectivity to the main Communication Manager server is lost.

Survivable core servers can be either Simplex or Duplex servers. The servers offer full Communication Manager functionality in the survivable mode, provided enough connectivity exists to other Avaya components. For example, endpoints, gateways, and messaging servers.

Standard Local Survivability

Standard Local Survivability (SLS) consists of a module built in to G430 Branch Gateway or G450 Branch Gateway to provide partial backup gateway controller functionality. The gateway provides the backup function when the connection with the primary controller is lost. To provide Communication Manager functionality when no link is available to an external controller, you can use a G430 Branch Gateway or G450 Branch Gateway without a local S8300E. Standard Local Survivability (SLS), Local Survivable Processor (LSP), and Branch Session Manager (BSM) are compatible with Edge Friendly Branch Survivability.

Support to tandem MIME for PIDF-LO

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

Support for Channel Type identification over ASAI to CTI application

Communication Manager 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

Chapter 3: Converged Networks

Voice over IP converged networks

Until recently, voice, video, and data were delivered over separate, single-purpose networks. A converged network brings voice, data, and video traffic together on a single IP network. VoIP technology from Avaya provides a cost-effective and flexible way of building enterprise communications systems through a converged network.

Some flexible elements of a converged network include:

- Separation of call control and switching functions. See *Separation of Bearer and Signaling Job*.
- Different techniques for handling data, voice, and FAX.
- Communications standards and protocols for different network segments.
- Constant and seamless reformatting of data for differing media streams.

Digital data and voice communications superimposed in a converged network compete for network bandwidth, or the total information throughput that the network can deliver. Data traffic requires significant network bandwidth for short periods of time, while voice traffic demands a steady, relatively constant transmission path. Data traffic can tolerate delays, while voice transmission degrades if delayed. Data networks handle data flow effectively. However, when digitized voice signals are added to the mix, networks must be managed differently to ensure constant, real-time transmission needed by voice.

Network assessment

Adding VoIP taxes network resources and performance because VoIP requires dedicated bandwidth and is more sensitive to network problems than data applications alone. Many customer IP infrastructures that appear to be stable and perform at acceptable levels might have performance and stability issues that create problems for Avaya VoIP Solutions. Therefore, Avaya cannot assure performance and quality without a network assessment even when a customer network seems ready to support full-duplex VoIP applications.

In Avaya, the network assessment services for VoIP consist of two phases:

- Basic Network Assessment: A high-level LAN and WAN infrastructure evaluation that determines the suitability of an existing network for VoIP.
- Detailed Network Assessment: A detailed analysis of the information gathered in the basic network assessment to provide functional requirements for the network to implement Avaya VoIP

.

For more information, see

- The network assessment offer in *Avaya Aura® Core Solution Description* .
- Avaya Communication Solutions and Integration (CSI) at http://csi.avaya.comfor a portfolio of consulting and engineering offers to plan and design voice and data networks.

For information about the Avaya network assessment policy, see http://netassess.avaya.com. This link is available only from within the Avaya corporate network.

Avaya gateways

The H.248 gateways include the G430 and G450 models. Both gateways have Media Module slots for analog, digital, loop start trunks, or T1/E1 capability. G430 and G450 also provide VoIP resources and announcement capabilities.

The following documents provide additional information about administration of Avaya gateways:

- *Administering Avaya G450 Branch Gateway*
- *Administering Avaya G430 Branch Gateway*
- *Avaya G450 Branch Gateway Overview and Specification*
- *Avaya G430 Branch Gateway Overview and Specification*
- *Avaya Branch Gateway G450 CLI Reference*
- *Avaya Branch Gateway G430 CLI Reference*

Avaya Aura® Media Server

The Avaya Aura® Media Server provides a large number of VoIP resources and announcement capabilities for large IP or cloud deployments.

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

IP trunks

The following sections describe the administration of IP trunks:

- SIP tunks

- H.323 trunks

SIP trunks

Session Initiation Protocol (SIP) is an endpoint-oriented messaging standard defined by the Internet Engineering Task Force (IETF). SIP trunking functionality is available on any Linux-based server. Linux servers function as Plain Old Telephone Service (POTS) gateways. These servers support name and number delivery among the various non-SIP endpoints, such as analog, DCP, or H.323 stations, and analog, digital or IP trunks that Communication Manager supports. These servers also support name and number delivery between SIP-enabled endpoints, such as the Avaya 4600-series SIP Telephones. In addition to calling capabilities, IP Softphone Release 5 and later include optional instant messaging client software, which is a SIP-enabled application. IP Softphone Release 5 also continues full support of the existing H.323 standard for call control. Avaya SIP Softphone Release 2 and later release fully support SIP for voice call control, instant messaging, and presence.

Communication Manager assigns two types of numbering to an incoming SIP trunk call:

- Private numbering: If the domain of the PAI, From, or Contact header in an incoming INVITE matches the authoritative domain of the called party network region.
- Public numbering: If the domain of the PAI, From, or Contact header in an incoming INVITE does not match the authoritative domain of the called party network region.

Public and private numbering plans are important when the incoming SIP trunk call is routed back over an ISDN trunk group.

ISDN defines numbering plans (NPI) and types of number (TON) within those plans.

Table 1: NPI and the values of TON within the plans

Number length	NPI=Public	NPI=Private	NPI=Unknown
Longest	TON=international	TON=Level 2	n/a
Middle	TON=national	TON=Level 1	n/a
Shortest	TON=Local	TON=Level 0	n/a
“don’t know”	TON=Unknown	TON=Unknown	TON=Unknown

If the caller does not know or does not want to specify the TON or NPI, Communication Manager can set that value to Unknown. When an incoming SIP call is routed to an ISDN network, Communication Manager always sets the TON to Unknown.

Creating a SIP trunk signaling group

Procedure

1. Type `add signaling-group n`, where *n* is the signaling group number.

   The system displays the Signaling Group screen.

2. In the **Group Type** field, type `sip`.
3. In the **Near-end Node Name** field, type the node name of the procr.

   The node names are administered on the Node Names screen and the IP Interfaces screen.
4. In the **Far-end Node Name** field, type the far end Session Manager name.

   Leave this field blank when the signaling group is associated with an unspecified destination.
5. In the **Near-end Listen Port** field, type the port number depending on the transport method.

   For example, enter 5060 for TCP/UDP and 5061 for TLS.
6. In the **Far-end Listen Port** field, enter the number entered in the **Near-end Listen Port** field.
7. In the **Far-end Network Region** field, enter a value from 1 to 250 or leave the field blank.

   Identify the network assigned to the far end of the trunk group. The far-end network region is used to obtain the codec set for negotiation of trunk bearer capability.
8. In the **Far-end Domain** field, type the name of the IP domain that is assigned to the far end of the signaling group.

   For example, to route Session Manager calls within an enterprise, the domain assigned to the proxy server is used. For external SIP calling, the domain name can be the name of the SIP service provider.

   Leave this field blank when you do not know the far-end domain.
9. In the **DTMF Over IP** field, specify the DTMF digits for transmission .

   The valid options for SIP signaling groups are:

   - **in-band**: All G711 and G729 calls pass DTMF in-band.
   - **out-of-band**: All IP calls pass DTMF out-of-band.
   - **rtp-payload**: RFC 2833 specifies this method. By default, RFC 2833 is the default value for newly added SIP signaling groups.

   For more information about the options, see *Avaya Aura® Communication Manager Screen Reference* .
10. Save the changes.
11. Type `add trunk-group n`, where *n* is the trunk group number.
12. In the **Group type** field, type `sip`.
13. In the **TAC** field, type the trunk access code number.
14. In the **Service type** field, type `tie`.
15. In the **Signaling Group** field, type the signaling group number that you configured earlier.

16. In the **Number of Members** field, type the number of members that you want to assign for the trunk.

    Enter a value in this field only when **member assignment** is auto.

17. Save the changes.

H.323 trunks

H.323 trunks use an ITU-T IP standard for LAN-based multimedia telephone systems. When IP-connected trunks are used, trunk groups can be defined as tie lines equivalent to ISDN-PRI between switches over an IP network.

H.323 trunk groups can be configured as:

- Tie trunks supporting ISDN trunk features such as DCS+ and QSIG
- Generic tie-trunks permitting interconnection with H.323 v2-compliant switches from other vendors
- Direct-inward-dial (DID) public trunks providing access to the switch for unregistered users

Preparing to administer H.323 trunks

Procedure

1. To busy out the signaling group, type **`busy signaling-group number`**.
2. Type **`change signaling-group number`**.

   The system displays the Signaling Group screen.

3. In the **Trunk Group for Channel Selection** field, type the trunk group number.

   If there is more than one trunk group assigned to this signaling group, enter the group that accepts incoming calls.

4. Save the changes.
5. Type **`release signaling-group number`** to release the signaling group.

Verifying customer options for H.323 trunking

About this task

Verify that H.323 trunking is set up correctly on the system-parameters customer-options screen. To make any changes to fields on this screen, go to the Avaya Support website at http://support.avaya.com.

Procedure

1. Type **`display system-parameters customer-options`**.

2. Go to the Optional Features screen.
3. Verify that the **G3 Version** field reflects the current version of Communication Manager.
4. Verify that the value in the **Maximum Administered H.323 Trunks** field is set to the number of trunks bought.

   The value must be greater than 0.
5. Verify that the **Maximum Administered Remote Office Trunks** field is set to the same value as the number of office trunks bought.

   This field is on page 2 of the Optional Features screen.
6. Go to the page that displays the **IP trunks** and **ISDN-PRI** fields.
7. Verify that **IP Trunks** and **ISDN-PRI** are enabled.

   If not, get a new license file.

QoS parameters

Four parameters on the IP-Options System-Parameters screen determine threshold Quality of Service (QoS) values for network performance. You can use the default values for these parameters, or you can change the default values to fit the needs of your network. See *Setting network performance thresholds*.

You can also administer additional QoS parameters, including defining IP Network Regions and specifying the codec type to be used. See Voice and Network quality administration on page 73.

Related links

Setting network performance thresholds on page 69

IP node names and IP addresses

Communication Manager uses node names to reference IP addresses throughout the system. Use the IP Node Names screen to assign node names and IP addresses to each node in the network with which this switch communicates through IP connections. The Node Names screen must be administered on each node in an IP network.

An IP node name can be any of these:

- Processor Ethernet (PE) IP Address
- Bridge or router IP Address
- SIP Trunk IP Address
- Avaya Application IP Address
- Messaging IP Address

Enter the Messaging name and IP address on the Messaging Node Names screen. Enter data for all other node types on the *IP Node Names* screen.

For H.323 connections, each Avaya Aura® Media Server IP Address on the local switch must also be assigned a node name and IP address on the *IP Node Names* screen.

Assign the node names and IP addresses in the network in a logical and consistent manner from the point of view of the network. Assign the names and addresses in the planning stages of the network. The names and addresses are available from the Avaya Support website at http://support.avaya.com.

Within the survivable Edge topology, the Local Survivable Processor (LSP) node names IP addresses are not the real IP addresses of the unreachable LSPs. Instead, they are local IP addresses assigned on main Communication Manager to access the remote servers. These IP addresses could be local IP's on the same subnetwork as the PROCR interface or loopback addresses internal to the Communication Manager server.

Assigning IP node names

About this task

You must assigns node names and IP addresses to each node in the network. Administer the IP Node Names screen on each call server or switch in the network.

Assign the node names and IP addresses logically and consistently across the entire network. Assign these names and addresses in the planning stages of the network. The names and addresses are available from the Avaya Support website at http://support.avaya.com.

Procedure

1. Type **`change node-names ip`**.

   The system displays the IP Node Names screen.

2. In the **Name** field, type the unique node names for the following:

   - Each Remote Office
   - Other IP gateways and hops

     The default node name and IP address is used to set up a default gateway. This entry is automatically present on the Node Names screen and cannot be removed.

     When the Node Names screen is saved, the system automatically alphabetizes the entries by node name.

3. In the **IP Address** field, type the unique ip address for each node name.
4. Save the changes.

Defining IP interfaces

Procedure

1. Type **`add ip-int`**.

   The system displays the IP Network Region screen.

2. Complete the fields using the information in *IP Network Region field descriptions*.
3. Save the changes.

Caution:

If you change 802.1p/Q on the IP Network Region screen, the format of the Ethernet frames is changes. 802.1p/Q settings in Communication Manager must match the settings in the interfacing elements in your data network.

Best Service Routing

Use H.323 trunks to implement Best Service Routing (BSR). This is an optional procedure. You can use H.323 trunks for polling, or for both polling and interflow. The additional network traffic is insignificant because polling requires only a small amount of data exchange. However, interflow requires a significant amount of bandwidth to carry the voice data. Depending on the other uses of the LAN or WAN and its overall utilization rate, voice quality could be degraded to unacceptable levels.

If H.323 trunks are used for BSR interflow, the traffic must be routed to a low-occupancy or unshared LAN WAN segment. You might also want to route internal interflow traffic, which has lower quality-of-service requirements, over H.323 trunks. You can route customer interflow traffic over circuit-switched tie trunks.

Administering an H.323 trunk

Procedure

1. Create one or more IP Codec sets that enable the appropriate transmission modes for the endpoints on the gateways.

   Note:

   You create the FAX, modem, TTY, and clear channel settings, including redundancy, on the second page of the IP Media Parameters screen. location must precede action.

2. Assign each codec set to the appropriate network region.
3. Assign the network region to the appropriate devices:
   - Avaya Aura® Media Server
   - G430 or G450 Branch Gateway

   .
4. If the G4xx Media Gateway or Avaya Aura® Media Server resources are shared among administered network regions, administer internetwork region connections.

Related links

Administering fax, TTY, modem, and clear-channel calls over IP trunks on page 60
Defining IP interfaces on page 28
IP codec sets on page 78
IP network regions on page 81
Manually interconnecting the network regions on page 101

H.323 trunk signaling group

Create a signaling group that is associated with H.323 trunks that connect this switch to a far-end switch. One or more unique signaling groups must be established for each far-end node to which this switch is connected through H.323 trunks.

Note:

The steps in this section address only those fields that are related to H.323 trunks. For information about the other fields, see *Administering Avaya Aura® Communication Manager*.

Creating an H.323 trunk signaling group

Procedure

1. Type `add signaling-group number`.

   The system displays the Signaling Group screen.

2. In the **Group Type** field, type `h.323`.

3. Leave the **Trunk Group for Channel Selection** field blank.

   After you create a trunk group, use the **change** command. Then type the trunk group number in the **Trunk Group for Channel Selection** field.

4. In the **T303 Timer** field, type the number of seconds that the system waits for a response from the far end before invoking Look Ahead Routing.

   The system displays the **T303 Timer** field when the **Group Type** field on the DS1 Circuit Pack screen is isdn-pri. The system also displays the **T303 Timer** when the **Group Type** field on the Signaling Group screen is h.323.

5. In the **H.245 DTMF Signal Tone Duration (msec)** field, specify the tone duration of DTMF tones sent in an H.245-signal message.

   The system displays the **H.245 DTMF Signal Tone Duration (msec)** field when the **DTMF over IP** field on the Signaling Group screen is set to **out-of-band**. The value of the **H.245 DTMF Signal Tone Duration (msec)** field can be either in the range 80 ms to 350 ms. The default value is blank.

6. In the **Near-end Node Name** field, type the node name for the PROCR IP interface on this switch.

   The node name must be administered on the Node Names screen and the IP Interfaces screen.

7. In the **Far-end Node Name** field, type the node name for the far-end PROCR IP Interface used for trunks assigned to this signaling group.

   The node name must be administered on the Node Names screen on this switch.

   Leave the **Far-end Node Name** field blank when the signaling group is associated with an unspecified destination.

8. In the **Near-end Listen Port** field, type an unused port number from the range 1719, 1720, or 5000 to 9999.

   Avaya recommends using port number 1720. If the **LRQ** field is y, type `1719`.

9. In the **Far-end Listen Port** field, enter the same number as the one in the **Near-end Listen Port** field.

   Leave the **Far-end Listen Port** field blank when the signaling group is associated with an unspecified destination.

10. In the **Far-end Network Region** field, enter a value between 1-250.

    Leave the field blank to select the region of the near-end node (PROCR). Identify the network assigned to the far end of the trunk group. The region is used to obtain the codec set used for negotiation of trunk bearer capability. If specified, this region is used for selection of a codec instead of the default region obtained from the PROCR used by the signaling group .

11. In the **LRQ Required** field, type `n` when the far-end switch is an Avaya product and **H.235 Annex H Required?** is set to `n`.

    Type `y` in one of the following situations:

    - The 235 Annex H Required? field is set to `y` or
    - The far-end switch requires a location request to obtain a signaling address in its signaling protocol.

12. In the **Calls Share IP Signaling Connection** field, type `y` for connections between Avaya equipment.

    Type `n` when the local or remote switch is not an Avaya switch.

13. In the **RRQ Required** field, type `y` when a vendor registration request is required.

14. In the **Bypass if IP Threshold Exceeded** field, type `y`.

    The system removes trunks assigned to this signaling group from service when IP transport performance falls below limits administered on the Maintenance-Related System Parameters screen.

15. In the **H.235 Annex H Required** field, type `y`.

    The **H.235 Annex H Required** field indicates whether the Avaya Aura® Communication Manager server requires H.235 amendment 1 with annex H protocol for authentication during registration.

16. In the **DTMF Over IP** field, specify the transmission of the DTMF digits.

    The valid options for SIP signaling groups are in-band and rtp-payload.

    The valid options for H.323 signaling groups are in-band, in-band-g711, out-of-band, and rtp-payload.

17. In the **Direct IP-IP Audio Connections** field, type `y`.

This option optimizes bandwidth resources and improves sound quality of voice over IP (VoIP) transmissions. For SIP Enablement Services (SES) trunk groups, this value helps in direct audio connections between SES endpoints.

18. In the **Link Loss Delay Timer** field, specify how long to hold the call state information in the event of an IP network failure or disruption.

    Communication Manager preserves calls and starts this timer at the onset of network disruption or signaling socket failure. If the signaling channel recovers before the timer expires, all call state information is preserved and the signaling channel is recovered. If the signaling channel does not recover before the timer expires, the system:

    - raises an alarm against the signaling channel
    - maintains all connections with the signaling channel
    - discards all call state information about the signaling channel

19. In the **IP Audio Hairpinning** field, type `y` to enable hairpinning for H.323 or SIP trunk groups.

    Using the **IP Audio Hairpinning** field entry, you have the option for H.323 and SES-enabled endpoints to be connected through the IP circuit pack in the server or switch, without going through the time division multiplexing (TDM) bus.

20. In the **Interworking Message** field, select a value that determines what message Communication Manager should send when an incoming ISDN trunk call is routed over a non-ISDN trunk group.

    Normally select the value PROGress, with which the public network can cut through the B-channel. The caller can then hear tones provided over the non-ISDN trunk, such as ringback or busy tone .

    Selecting the value ALERTing causes the public network in many countries to play ringback tone to the caller. Select this value only if the DS1 is connected to the public network, and it is determined that callers hear silence rather than ringback or busy tone when a call incoming over the DS1 is routed to a non-ISDN trunk.

21. In the **DCP/Analog Bearer Capability** field, set the information transfer capability in a bearer capability IE of a setup message to **speech** or **3.1kHz**.

    The default value is 3.1kHz. The default value provides 3.1kHz audio encoding in the information transfer capability. Selecting the value of speech provides speech encoding in the information transfer capability.

22. If using DCS, go to the Administered NCA TSC Assignment page of this screen.

    To enter NCA TSC information on this screen, see *Avaya Aura® Communication Manager Screen Reference*.

23. Save the changes.

Creating a trunk group for H.323 trunks

About this task

Use this procedure to create a new trunk group for H.323 trunks. Each H.323 trunk must be a member of an ISDN trunk group and associated with an H.323 signaling group.

Note:

The following steps address only those fields that are specifically related to H.323 trunks. For information about the other fields, see *Administering Avaya Aura® Communication Manager*.

Procedure

1. Type **`add trunk-group next`**.

   The system displays the Trunk Group screen.
2. In the **Group Type** field, type `isdn`.
3. In the **Carrier Medium** field, type `H.323`.
4. In the **Service Type** field, type `tie`.
5. In the **TestCall ITC** field, type `unre`.
6. In the **TestCall BCC** field, type `0`.
7. In the **Codeset to Send Display** field, type `0`.
8. if the far end comprises non-Avaya endpoints, change the **Outgoing Display** field.
9. Go to the Trunk Features page of the screen.
10. Verify the values in the **Send Name**, **Send Calling Number**, and **Send Connected Number** fields.

    If these fields contain y, the system accesses the ISDN Numbering - Public/Unknown Format screen or the ISDN Numbering - Private screen based on the **Format** field. The system uses information from these screens to construct the actual number to be sent to the far end.
11. To add a second signaling group, go to the Group Member Assignments page of this screen.

    Note:

    Each signaling group can support up to 31 trunks. For more trunks between two switches, add a second signaling group with different listen ports. Add the trunks to the existing or second trunk group.
12. In the **Port** field, type `ip`.

    When the screen is submitted, this value is automatically changed to a T number.
13. In the **Name** field, type a 10-character name to identify the trunk.

14. In the **Sig Grp** field, type the number for the signaling group associated with this H.323 trunk.

Modifying the H.323 trunk signaling group

About this task

Update values in the Signaling Group screen to add a trunk group number to the **Trunk Group for Channel Selection** field.

Procedure

1. Type **`busy signaling-group number`** to busy out the signaling group.
2. Type **`change signaling-group number`**.

   The system displays the Signaling Group screen.
3. In the **Trunk Group for Channel Selection** field, type the trunk group number.

   When more than one trunk group is assigned to a signaling group, enter the group that accepts incoming calls.
4. Save the changes.
5. Type **`release signaling-group number`** to release the signaling group.

Dynamic generation of private/public calling party numbers

Often, a private Calling Party Number (CPN) is generated for calls within a network. However, a public CPN is required for calls that route through the main network switch to the PSTN.

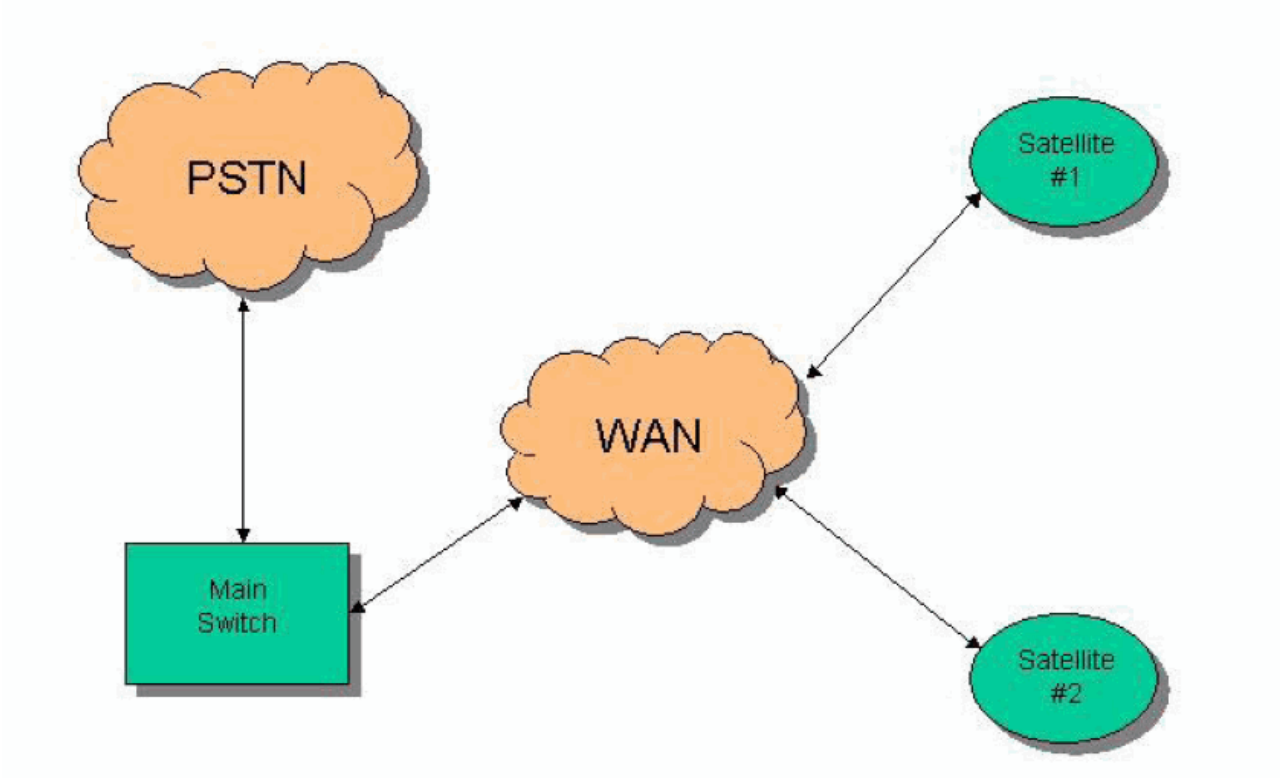


Figure 5: Private/public calling party numbers (CPN)

In this network, the customer wants to use internal numbering among the nodes of the network, for example, a 4-digit Uniform Dial Plan (UDP). However, when any node dials the PSTN, the call must be routed to the PSTN through the main switch.

On page 2 of the ISDN Trunk Group screen, set the **Numbering Format** field to private or unk-pvt. With the value unk-pvt, the number is encoded as an unknown type of number, however, the Numbering-Private Format screen is used to generate the actual number.

Note:

In this scenario, IP trunks function as ISDN trunks.

In the network example, the system only generates a private CPN if the caller dials a private level 0, 1, or 2, or unknown unk-unk number. If the caller dials a public number, the system generates a public CPN. You must fill the Numbering-Private Format and Numbering-Public/Unknown Format forms appropriately. You must then set the IP trunk groups on the two satellites to use private or unk-pvt numbering format for their CPNs.

Note:

You can designate the type of number for an outgoing call as Private level 0, 1, or 2 either on the AAR Analysis screen or the Route Pattern screen. You can designate the type of number as unk-unk or unknown only on the Route Pattern screen. If you are using UDP, then you must use the Unknown Type of Number.

The default Call Type on the AAR Analysis screen is aar. For historical reasons, aar maps to a public numbering format. Therefore, you must change the Call Type for calls within your network from aar to a private or unk-unk type of number. For a UDP environment, you must set the Numbering Format to unk-unk on the Route Pattern screen.

Avaya IP phones

The following sections describe the installation and administration of Avaya IP telephones:

- IP Softphones on page 36
- Avaya IP telephones on page 39

IP softphones

IP softphones operate on a personal computer equipped with Microsoft Windows and TCP/IP connectivity through Communication Manager. Avaya offers the following softphone applications:

- IP softphone for any telephone user
- IP Agent for call center agents
- Softconsole for console attendants
- Avaya one-X® Communicator
- SIP softphone
- one-X Portal as a software-only telephone

IP softphones can be configured to operate in any of the following modes:

- Road-warrior mode: Consists of a personal computer running the Avaya IP Softphone application and Avaya iClarity IP Audio with a single IP connection to an Avaya server or gateway.
- Telecommuter mode: Consists of a personal computer running the Avaya IP Softphone application with an IP connection to the server and a standard telephone with a separate PSTN connection to the server.
- Shared Control mode: Provides a registration endpoint configuration using which an IP Softphone and a non-softphone telephone can be in service on the same extension at the same time. In this new configuration, both the softphone and the telephone endpoint provide call control. The telephone endpoint provides the audio.

Documentation on how to set up and use the IP softphones is included on the CD-ROM containing the IP softphone software. For information about administering Communication Manager to support IP softphones, see *Administering Avaya Aura® Communication Manager*.

This section focuses on administration for the trunk side of the Avaya IP Solutions offer and a checklist of IP softphone administration. For information about administering IP softphones, see *Administering Avaya Aura® Communication Manager*.

The two main types of IP Softphone configurations are:

- Administering a Telecommuter Telephone on page 37
- Administering a Road-warrior telephone on page 38

Communication Manager can distinguish between various IP stations at RAS using the product ID and release number sent during registration. An Avaya IP phone can register when:

- a number of stations are present in the network with the same product ID and the same or lower release number
- the number of stations is less than the administered system capacity limits

System limits are based on the number of simultaneous registrations. A license is required for each station that must be IP softphone enabled.

Administering a Telecommuter telephone

About this task

The Telecommuter phone uses two connections, one to the personal computer over the IP network and the other to the telephone over the PSTN. IP Softphone personal computer software handles the call signaling. With IP Softphone R5 or greater, iClarity is automatically installed to handle voice communications.

Note:

The System Parameters Customer Options screen is display only. Use the **`display system-parameters customer-options`** command to review the screen. The License File controls the system software release, the Offer Category, features, and capacities. With the init login, you cannot change the customer options, offer options, or special applications screens.

Procedure

1. Type **`display system-parameters customer-options`** and press `Enter`.

   The system displays the System Parameters Customer Options screen.

2. Verify that IP Softphone is enabled.

   Review the following fields on the screen:

   - In the **Maximum Concurrently Registered IP Stations** field, the value must be greater than 0 and less than or equal to the value for Maximum Ports.

     This field identifies the maximum number of IP stations that are simultaneously registered, not the maximum number that are simultaneously administered.

   - In the **IP Stations** field, the value must be y.
   - In the **Product ID** field, for new installations, IP Soft, IP Telephone, IP Agent, and IP ROMax, the system displays the product IDs automatically.

     This field is a 10-character field with any character string.

   - In the **Rel. (Release)** field, check the release number.

- In the **Limit** field, check the value.

  The default setting is the maximum value based on the **Concurrently Registered Remote Office Stations** field on page 1 of the System Parameters Customer Options screen.

3. Type **`add station next`** and press `Enter`.

   The system displays the Station screen.

4. Add a DCP station, or change an existing DCP station.
5. In the **Type** field, type the telephone model.
6. In the **Port** field, type `x` for a virtual phone or the port number of an existing telephone.
7. In the **Security Code** field, type the station security code that is assigned to the extension as a password.
8. In the **IP Softphone** field, type `y`.
9. Go to page 2, and verify whether the **Service Link Mode: as needed** field is set as shown.
10. Install the IP Softphone software on the personal computer of the user.

Administering a road warrior telephone

About this task

The softphone application runs on a personal computer that is connected over an IP network. In the road warrior mode, the application uses one channel for call control signaling and one channel for voice.

Note:

The System Parameters Customer Options screen is display only. Use the **`display system-parameters customer-options`** command to review the screen. The License File controls the system software release, the Offer Category, features, and capacities. With the init login, you cannot change the customer options, offer options, or special applications screens.

Procedure

1. Type **`display system-parameters customer-options`**.
2. Verify that IP softphone is enabled.

   Go to the appropriate pages on the System Parameters Customer Options screen to review the following fields:

   - In the **Maximum Concurrently Registered IP Stations** field, the value must be greater than 0.
   - In the **IP Stations** field, the value must be y.
   - In the **Product ID** field, for new installations, IP Soft, IP Telephone, IP Agent, and IP ROMax, the system displays the product IDs automatically.

     The **Product ID** field is a 10-character field with any character string.

- In the **Rel. (Release)** field, check the release number.
- In the **Limit** field, check the default value.

  The default value is 1.

3. Type **add station next** and press Enter.

   The system displays the Station screen.
4. Add a DCP station or change an existing DCP station.
5. In the **Type** field, type the telephone model to use, such as 6408D.
6. In the **Port** field, type x if virtual, or the port number of an existing telephone.

   For an IP Softphone, type IP.
7. In the **Security Code** field, type the station security code that is assigned to the extension as a password.
8. In the **IP Softphone** field, type y.
9. Go to page 2, Service Link Mode: as-needed.

   Install the IP Softphone software on the personal computer of the user. With the IP Softphone Release 2 or later, iClarity is automatically installed.

Avaya IP telephones

The Avaya line of digital business telephones uses Internet Protocol (IP) technology with Ethernet line interfaces and has downloadable firmware.

IP Telephones provide support for dynamic host configuration protocol (DHCP) and either Trivial File Transfer Protocol (TFTP) or Hypertext Transfer Protocol (HTTP) over IPv4/UDP. These protocols enhance the administration and servicing of the telephones.

For information about feature functionality of the IP telephones, see the *Avaya Aura® Communication Manager Hardware Description and Reference*, or the appropriate IP Telephone user guides.

For more information about installing and administering Avaya IP telephones, see

- *4600 Series IP Telephone Installation Guide*
- *4600 Series IP Telephone LAN Administrator's Guide*
- *Avaya one-X Deskphone Edition 9600 Series IP Telephone Installation and Maintenance Guide*
- *Avaya one-X Deskphone Edition 9600 Series IP Telephones Administrator Guide*
- *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide*
- *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Administrator Guide Release 1.0*

For more information about IP Wireless Telephone Solutions, go to http://support.avaya.com.

4600-series IP telephones

The 4600-series IP telephone product line possesses a number of shared model features and capabilities. All models also feature:

- Downloadable firmware
- Automatic IP address resolution through DHCP
- Manual IP address programming

The 4600-series IP Telephone product line includes the following telephones:

- Avaya 4601 IP telephone
- Avaya 4602 and 4602SW IP telephone
- Avaya 4610SW IP telephone
- Avaya 4620 and 4620SW IP telephone
- Avaya 4622SW IP telephone
- Avaya 4622 IP telephone
- Avaya 4625 IP telephone
- Avaya 4630SW IP Screenphone
- Avaya 4690 IP conference telephone

Support for SIP-enabled applications can be added to several of these IP telephones by a model-specific firmware update. For more information, see the Avaya Firmware Download website .

96x1-series IP telephones

The 96x1-series IP telephone product line possesses a number of shared model features and capabilities. All models feature:

- Downloadable firmware
- Automatic IP address resolution through DHCP
- Manual IP address programming

The 96x1-series IP telephone product line includes the following telephones:

- Avaya 9611 H.323 and SIP deskphones for everyday users
- Avaya 9621 H.323 and SIP deskphones for essential users
- Avaya 9641 H.323 and SIP deskphones for essential users
- Avaya 9610 IP telephone for walkup users

9600-series IP telephones

The 9600-series IP telephone product line possesses a number of shared model features and capabilities. All models feature:

- Downloadable firmware
- Automatic IP address resolution through DHCP
- Manual IP address programming.

The 9600-series IP telephone product line includes the following telephones:

- Avaya 9610 IP telephone for Walkup users
- Avaya 9620 IP telephone for the Everyday user
- Avaya 9630 IP telephone with advanced communications capabilities
- Avaya 9640 IP telephone with advanced communications capabilities, color display
- Avaya 9650 IP telephone for the executive administrative assistant
- Avaya 9608 IP telephone
- Avaya 9611 IP telephone
- Avaya 9621 IP telephone
- Avaya 9641 IP telephone

Support for SIP-enabled applications can be added to several of these IP telephones through a model-specific firmware update. See the Avaya Firmware Download website for more information.

1600-series IP telephones

The 1600-series IP Telephone product line possesses a number of shared model features and capabilities. All models feature:

- Downloadable firmware
- Automatic IP address resolution through DHCP
- Manual IP address programming

The 4600-series IP Telephone product line includes the following telephones:

- Avaya 1603 IP Deskphone for walkup users
- Avaya 1608 IP Deskphone for the everyday user
- Avaya 1616 IP Deskphone for navigational use

Note:

Support for SIP-enabled applications can be added to several of these IP telephones through a model-specific firmware update. For more information, see the Avaya Firmware Download website.

J1xx-series IP telephones

The J1xx-series IP telephone product line possesses a number of shared model features and capabilities. All models feature:

- Downloadable firmware
- Automatic IP address resolution through DHCP
- Manual IP address programming.

The J1xx-series IP telephone product line includes the following telephones:

- Avaya J129 IP telephone
- Avaya J139 IP telephone
- Avaya J159 IP telephone
- Avaya J179 IP telephone
- Avaya J189 IP telephone

Support for SIP-enabled applications can be added to several of these IP telephones through a model-specific firmware update. See the Avaya Firmware Download website for more information.

IP telephone hardware and software

IP telephones are shipped from the factory with operational firmware installed. Some system-specific software applications are downloaded from a TFTP or HTTP server through automatic power-up or reset. The IP telephones search and download new firmware from the file server before attempting to register with Communication Manager.

During a Communication Manager upgrade, any data in the `/tftpboot` directory is overwritten with new software and firmware.

The software treats the 4600-series and 9600-series IP telephones as any new station type, including the capability to **`list/display/change/duplicate/remove station`**.

Audio capability for the IP telephones requires the presence of G4xx Media Gateway or Avaya Aura® Media Server. Either of the circuit packs provide hairpinning and IP to IP direct connections. Using a media processor resource conserves TDM bus and timeslot resources and improves voice quality.

To register H.323 endpoints without TTS, at least one connected network region of the IP station must have a PROCR.

Administering Avaya IP telephones

About this task

IP Telephones Release 1.5 or later use a single connection, and you only need to administer the station type.

Procedure

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

   The system displays the Station screen.

2. In the **Type** field, type the IP Telephone 4600-series model number, such as 4624.

   The following phones are administered with an alias:

   - 4601: Administer as a 4602.
   - 4602SW: Administer as a 4602.
   - 4690: Administer as a 4620.

3. In the **Port** field, type `x` or `IP`.

   Note:

   A 4600-series IP Telephone is always administered as an X port. After successful registration by the system, a virtual port number is assigned. Note that a station that is registered as unnamed is not associated with any logical extension or administered station record.

4. For IP Telephones Release 2 or earlier with dual-connection architecture, complete the following fields:

   - In the **Media Complex Ext** field, type the H.323 administered extension.
   - In the **Port** field, type `x`.

5. Save the changes.

Hairpinning, shuffling, and direct media

Communication Manager can shuffle or hairpin call path connections between two IP endpoints. Shuffling is done by rerouting the voice channel away from the usual TDM bus connection and creating a direct IP-to-IP connection. Shuffling and hairpinning are similar because these techniques maintain connection and conversion resources that might not be needed. Connection and conversion resources are preserved depending on the compatibility of the endpoints that are attempting to interconnect.

Shuffling and hairpinning techniques differ in the way that these techniques bypass the unnecessary call-path resources.

Shuffled or hairpinned connections:

- Conserve channels on the G4xx Media Gateway and Avaya Aura® Media Server.
- Bypass the TDM bus, conserving timeslots.
- Improve voice quality by removing unnecessary VoIP-TDM-VoIP conversions.

Shuffling releases more resources on the G4xx Media Gateway and Avaya Aura® Media Server than hairpinning does. Therefore, Communication Manager first checks both endpoints to determine whether Communication Manager meets the criteria for using a shuffled audio connection. If the shuffling criteria are not met, Communication Manager routes the call according to the criteria for hairpinning, if hairpinning is enabled. If hairpinning is not enabled, Communication Manager routes the call to the TDM bus. Both endpoints must connect through the same G4xx Media Gateway and Avaya Aura® Media Server for Communication Manager to shuffle or hairpin the audio connection.

For information on interdependencies that enable hairpinning and shuffling audio connections, see *Hairpinning and shuffling administration interdependencies*. For Network Address Translation (NAT), see *Network Address Translation*.

Hardware and endpoints

The G4xx Media Gateway or Avaya Aura® Media Server is required for shuffling or hairpinning audio connections.

You can administer the following endpoint types for hairpinning or shuffling:

- All Avaya IP stations
- Stations of other vendors that are compatible with H.323

Shuffled audio connections

Shuffling an audio connection between two IP endpoints means rerouting the voice channel away from the usual TDM bus connection and creating a direct IP-to-IP connection. Shuffling saves resources such as G4xx Media Gateway or Avaya Aura® Media Server channels and improves voice quality by bypassing transcoding. Both endpoints must be capable of shuffling.

Communication Manager uses the following criteria to determine whether a shuffled audio connection is possible:

- A point-to-point voice connection exists between two endpoints.
- No other active call on either endpoint, including in-use or held calls, requires TDM connectivity. For example, applying tones, announcement, conferencing, and others.
- The endpoints are in the same network region or in different, interconnected regions.
- Both endpoints or connection segments are administered for shuffling by setting the **Direct IP-IP Audio Connections** field to `y` for shuffled IP calls to use a public IP address by default.
- If the **Direct IP-IP Audio Connections** field is `y`, during registration the endpoint might indicate that it does not support audio shuffling. In this scenario, the a call cannot be shuffled. If the **Direct IP-IP Audio Connections** field is `n`, during registration the endpoint might indicate that it can support audio shuffling. The calls to that endpoint cannot be shuffled, giving precedence to the endpoint administration.
- The rules for Internetwork region connection management on page 54 are met.
- At least one common codec is present between the endpoints involved and the Inter-network region Connection Management codec list.
- The endpoints have at least one codec in common as shown in the current codec negotiations between the endpoint and the switch.
- Both endpoints can connect through the same G4xx Media Gateway or Avaya Aura® Media Server.

Examples of shuffling

Shuffling within the same network region

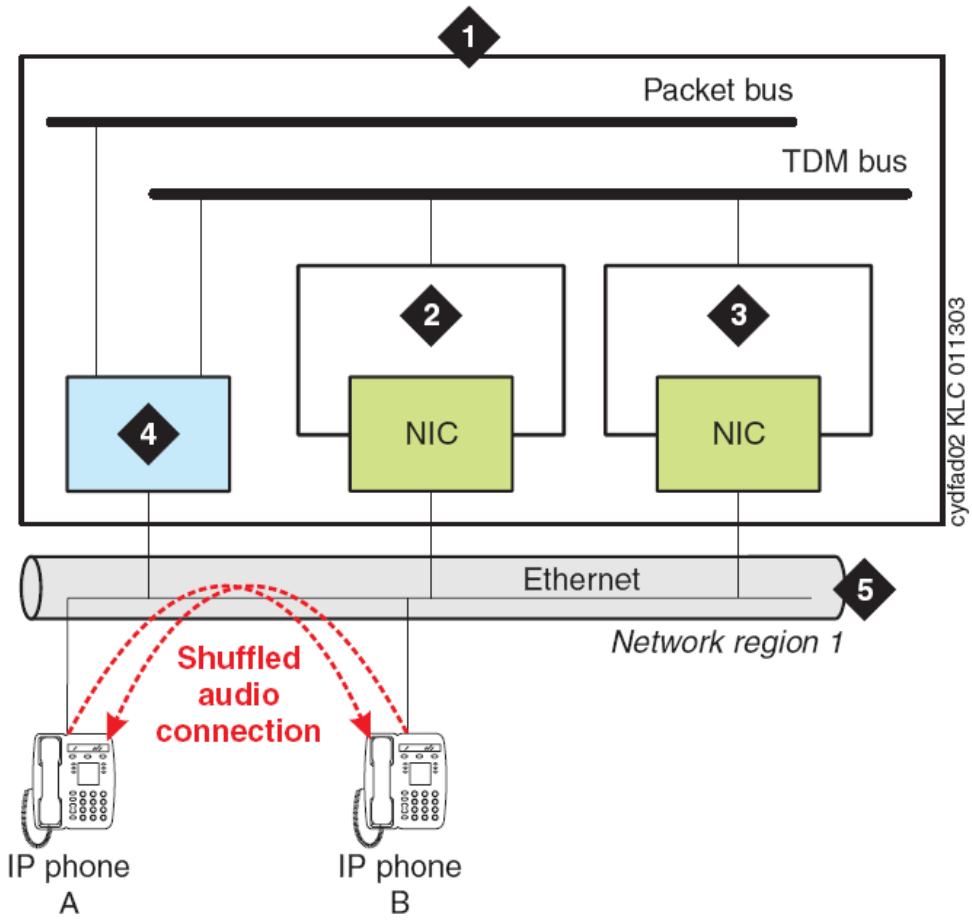


Figure 6: Shuffled audio connection between IP endpoints in the same network region

Number	Description
1	Avaya server
2	G4xx Media Gateway
3	G4xx Media Gateway and Avaya Aura® Media Server
4	PROCR
5	LAN/WAN segment administered in Communication Manager as network region 1

Shuffling within the same network region on page 45 is a schematic of a shuffled connection between two IP endpoints within the same network region. After the call is shuffled, the IP Media Processors are out of the audio connection and free to serve other media connections.

Determining whether an endpoint supports shuffling

About this task

To determine whether an endpoint supports audio shuffling. make a test call from an endpoint that supports shuffling to another endpoint whose shuffling capability is unknown.

Procedure

1. On the station screen, administer the **Direct IP-IP Audio Connections** field on page 2 as `y` (yes) for both endpoints.

   Use the **`change station extension`** command to reach the station screen for each endpoint.

2. From the endpoint that can support shuffling, make a call to the endpoint that you are testing.

   Wait for 2 minutes.

3. On SAT, type **`status station`** *extension*, where *extension* is the administered extension of the endpoint that you are testing, and press `Enter`.

   The system displays the Station screen for this extension.

4. In the GENERAL STATUS section of page 1, note the **Port** field value .

5. Scroll to page 4.

   In the AUDIO CHANNEL section, note the value in the **Audio** field in the Switch Port column.

   - If the values are the same, the endpoint supports shuffling.

     Administer the **Direct IP-IP Audio Connections** field as `y` (yes).

     To find the **Direct IP-IP Audio Connections** field, use the **`change station extension`** command and scroll to page 2.

     If the values are different, then the endpoint cannot shuffle calls.

     Administer the **Direct IP-IP Audio Connections** field as `n` (no).

Shuffling between different network regions

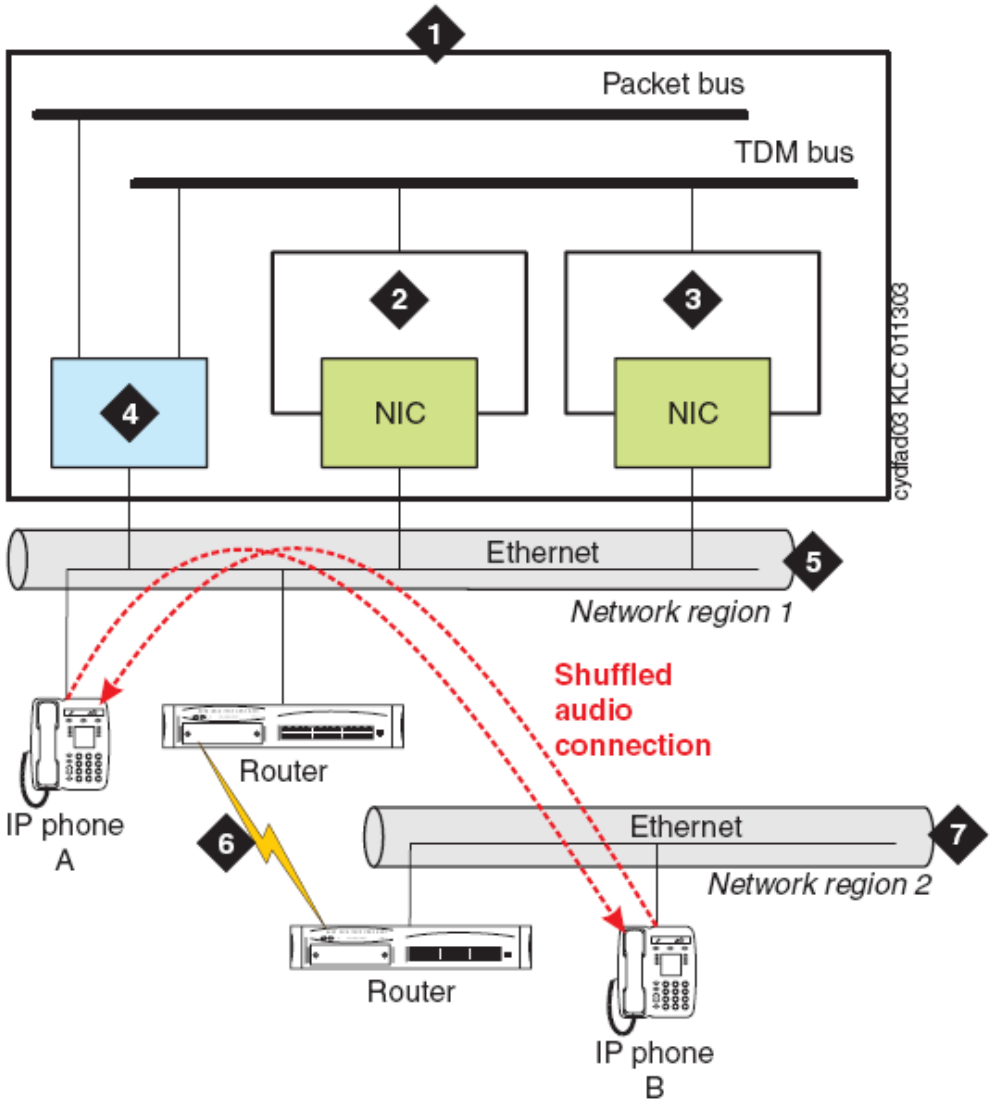


Figure 7: Shuffled audio connection between IP endpoints in different network regions

Number	Description
1	Avaya server
2	G4xx Media Gateway and Avaya Aura® Media Server
3	G4xx Media Gateway and Avaya Aura® Media Server
4	PROCR

Table continues…

Number	Description
5	LAN/WAN segment administered in Communication Manager as network region 1
6	IP voice packet path between LAN routers
7	LAN/WAN segment administered in Communication Manager as network region 2

Figure 7: Shuffled audio connection between IP endpoints in different network regions on page 47 is a schematic of a shuffled audio connection between two IP endpoints that are in different network regions that are interconnected. The internetwork region connection management rules are met for these different network regions. After the call is shuffled, both Media Processors are bypassed, making those resources available to serve other media connections. The voice packets from IP endpoints flow directly between LAN routers.

Administrable loss plan

Two-party connections between IP endpoints are not subject to the administrable loss plan of the switch. Due to this exemption, audio levels do not change when a two-party call changes from the TDM bus to a shuffled or hairpinned connection. Although IP endpoints can be assigned to administrable loss groups, the switch is only able to change loss on IP Softphone calls including circuit-switched endpoints. Conference calls with three parties or more are subject to the administrable loss plan, regardless of whether the calls involve IP endpoints or not.

Hairpinning and shuffling administration interdependencies

The following table summarizes the Communication Manager interdependencies that enable shuffling audio connections.

Note:

To use shuffling with either Category A or B features, the **Software Version** field must be `R9` or later. Use the **`list configuration software-versions`** command to view the **Software Version** field.

Table 2: Shuffling administration

Administration screen	Required customer options	Other interactions
Station	IP StationsRemote Office	Shuffling is available only for the following endpoints: • Avaya IP telephone Release 2 • Avaya IP Softphone Release 2 or later
Signaling group	H.323 Trunks	
Inter network region	H.323 TrunksIP Stations Remote Office	User login must have features permissions.

Table continues…

Administration screen	Required customer options	Other interactions
Feature-Related System Parameters	H.323 TrunksIP Stations Remote Office	

The fields listed in the Required customer options column must be enabled through the License File. To determine if these customer options are enabled, use the **`display system-parameters customer-options`** command. If any fields listed in the Required customer options column are not enabled, then:

- The field for shuffling are not displayed.
- In the Inter Network Region Connection Management screen, the second page with the region-to-region connection administration does not display.

Although fully H.323v2-compliant products of other vendors have shuffling capability, you must test the endpoints before administering such endpoints for shuffling. See Determining whether an endpoint supports shuffling on page 46.

SIP Early Direct Media

Communication Manager supports SIP Early Direct Media for Session Initiation Protocol (SIP) calls. Direct Media signals the direct talk path between SIP endpoints before a call connects.

Direct Media provides the following enhancements to SIP calls:

- Eliminates shuffling of SIP calls after the 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 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.

Related links

Administering shuffling in network regions on page 54

Preparing to enable SIP Early Direct Media

Procedure

1. Ensure that the call originator is SIP.

   If the call originator is not SIP, Communication Manager does not apply SIP Early Direct Media to the call.

2. Set the **Direct IP-IP Audio Connections** and **Initial IP-IP Direct Media** fields in the SIP signalling group screen of the originating SIP User Agent to y.
3. Ensure that the call-originating party does not have a call on hold.

Note:

If you do not meet with the prerequisites for SIP Early Direct Media, Communication Manager allocates media processors and shuffles the call after the connection is established.

Network Address Translation

Network address translation (NAT) is a function, typically in a router or firewall, by which an internal IP address is translated to an external IP address. The terms internal and external are generic, ambiguous and more specifically defined by the application. For example, the most common NAT application is to facilitate communication from hosts on private networks to hosts on the public Internet. In such a case, the internal addresses are private addresses, and the external addresses are public addresses.

Note:

This common NAT application does not use a web proxy server, which would be an entirely different scenario.

Another common NAT application is for some VPN clients. The internal address in VPN clients is the physical address, and the external address is the virtual address. This physical address does not have to be a private address, as the subscriber can pay for a public address from the broadband service provider. Regardless of the nature of the physical address, the physical address cannot be used to communicate back to the enterprise network through a VPN tunnel. After the tunnel is established, the enterprise VPN gateway assigns a virtual address to the VPN client application on the enterprise host. This virtual address is part of the enterprise IP address space, and it must be used to communicate back to the enterprise network.

The application of the virtual address varies among VPN clients. Some VPN clients integrate with the operating system so that packets from IP applications on the enterprise host are sourced from the virtual IP address. Examples of IP applications include FTP or telnet. The IP applications inherently use the virtual IP address. With other VPN clients, the IP applications do not use the virtual IP address. Instead, IP applications on the enterprise host inherently use the physical IP address, and the VPN client performs a NAT to the virtual IP address. This NAT is the same as the translation done with a router or firewall.

Types of Network Address Translation

Static 1-to-1 NAT

In Static 1-to-1 NAT, every internal address has an external address, with a static 1-to-1 mapping between internal and external addresses. Static 1–to-1 NAT is the simplest, yet least efficient type of NAT in terms of address preservation because every internal host requires an external IP address. This limitation is often impractical when the external addresses are public IP addresses. Sometimes the primary reason for using NAT is to preserve public IP addresses. Hence, two other types of NAT, many-to-1 and many-to-a-pool, are available for preserving public IP addresses.

Dynamic many-to-1 NAT

In Dynamic many-to-1 NAT, many internal addresses are dynamically translated to a single external address. Multiple internal addresses can be translated to the same external address

when the TCP/UDP ports are translated in addition to the IP addresses. This type of address translation is known as network address port translation (NAPT) or port address translation (PAT). The external server receives multiple requests from a single IP address, but from different TCP/UDP ports. The NAT device remembers which internal source ports were translated to which external source ports.

In the simplest form of many-to-1 NAT, the internal host must initiate the communication to the external host, which then generates a port mapping within the NAT device. The external host can then reply to the internal host. With this type of NAT, in its simplest form, the external host cannot generate a port mapping to initiate communication with the internal host, and without initiating communication, there is no way to generate port mapping. This condition does not exist with 1-to-1 NAT, as there is no mapping of ports.

Dynamic many-to-a-pool NAT

Many-to-a-pool NAT combines some of the characteristics of both 1-to-1 and many-to-1 NAT. The idea behind many-to-a-pool NAT is that 1-to-1 mapping is avoided, but too many internal hosts are present to use a single external address. Therefore, a pool of multiple external addresses is used for NAT. Enough external addresses are available in the pool to support all internal hosts. However, the number of internal hosts is greater than the number of pool addresses.

Issues between NAT and H.323

Some of the hurdles that NAT presents to H.323 include:

- H.323 messages, which are part of the IP payload, have embedded IP addresses in them.

  NAT translates the IP address in the IP header, but not the embedded addresses in the H.323 messages. This problem can be and has been addressed with H.323-aware NAT devices. The problem has also been addressed with Communication Manager 1.3 and later versions of the NAT feature.

- When an IP telephone registers with the gatekeeper or call server, the IP address of that endpoint must stay the same for the duration of the registration.

  This hurdle rules out almost all current implementations of many-to-a-pool NAT.

- TCP/UDP ports are involved in all aspects of IP telephony, including endpoint registration, call signaling, and RTP audio transmission.

  These ports must remain unchanged throughout an event, during the registration, or during a call. Also, the gatekeeper must have, ahead of time, the ports that will be used by the endpoints for audio transmission, and these ports can vary for every call. These requirements complicate how H.323 works with port address translation (PAT), which rules out most current implementations of many-to-1 and many-to-a-pool NAT.

Communication Manager NAT Shuffling feature

With the Communication Manager NAT Shuffling feature, IP telephones and IP Softphones can work behind a NAT device. This feature was available before release 1.3, but it did not work with shuffled calls activated by enabling Direct IP-IP Audio. The NAT feature now works with shuffled calls.

Terms

The following terms are used to describe the NAT Shuffling feature:

- Native Address: The original IP address configured on the device, also known as the internal address.
- Translated Address: The IP address after it has gone through NAT, as seen by devices on the other side of the translation, also known as external address.
- Gatekeeper: The Avaya device that is handling call signaling which is processor Ethernet.
- Gateway: The Avaya device that is handling media conversion between TDM and IP. The device can be any of the following branch gateways:
  - G450
  - G430

With this feature, Communication Manager keeps track of the native and translated IP addresses for every IP station such as an IP telephone or IP Softphone. If an IP station registration displays with different addresses in the IP header and the RAS message, the call server stores the two addresses. The call server also alerts the station that NAT occurred.

This feature works with static 1-to-1 NAT. This feature does not work with NAPT, so the TCP/UDP ports sourced by the IP stations must not be changed. Consequently, this feature does not work with many-to-1 NAT. This feature works with many-to-a-pool NAT if the translated address of a station remains constant for when the station is registered, without port translation.

The NAT device must perform plain NAT, not H.323-aware NAT. Any H.323-aware feature in the NAT device must be disabled, so that two independent devices do not try to compensate for H.323 simultaneously.

Rules

The following rules govern the NAT Shuffling feature:

- When **Direct IP-IP Audio** is enabled and a station with NAT and a station without NAT communicate, the translated address is used. The **Direct IP-IP Audio** parameters are configured on the SAT ip-network-region screen. **Direct IP-IP Audio** is enabled by default.
- When two stations with NAT communicate, the native addresses are used when Direct IP-IP Audio is administered with `Yes` or `Native (NAT)`. The translated addresses are used when Translated (NAT) is specified.
- The Gatekeeper and Gateway must not be enabled for NAT so that these devices can be assigned to any network region.

Shuffling

You can administer shuffled connections:

- Independently for systemwide applicability
- Within a network region
- At the user level

Checklist for administering shuffling

Use this checklist while administering shuffling at any of these levels:

- System level
- Network region level
- IP trunks level
- IP endpoints level

No.	Task	Description	✔
1	Administer shuffling for the system from the Feature-Related System Parameters screen.	See Administering hairpinning and shuffling at the system-level on page 53.	
2	Administer shuffling for the network region level from the Network Region screen.	See Inter-network region connection management on page 54.	
3	Administer shuffling for IP trunks from the Signaling Group screen.	See Administering H.323 trunks for hairpinning and shuffling on page 56.	
4	Administer shuffling for IP endpoints from the Station screen.	See Administering IP endpoints for hairpinning and shuffling on page 56.	

Administering shuffling at the system level

Before you begin

Ensure that the following fields on the Customer Options screen are set to **y**:

- **IP Stations**
- **H.323 Trunks**
- **Remote Office**

If the **IP Stations**, **H.323 Trunks**, and **Remote Office** fields are set to **n**, the **Direct IP-IP Audio Connections** fields do not display.

About this task

You can administer shuffling as a system-wide parameter.

Procedure

1. On the SAT screen, type `change system-parameters features` and press `Enter`.

   The system displays the Feature-Related System Parameters screen.

2. Go to the page with IP PARAMETERS and set the **Direct IP-IP Audio Connections** field to **y**.

   When you set the **Direct IP-IP Audio Connections** field to **y**, shuffled IP calls use a public IP address by default.

3. Save the changes.

Internetwork region connection management

Shuffling endpoints or media processing resources in any given network are independently administered for each network region. A matrix is used to define the connections between pairs of regions.

The matrix specifies which regions are valid for resource allocation when resources in the preferred region are unavailable. When a call exists between two IP endpoints in different regions, the matrix specifies whether those two regions can be connected directly.

Administering shuffling in network regions

Before you begin

Ensure that you set the following fields on the Optional Features screen to `y`:

- **IP Stations**
- **H.323 Trunks**
- **Remote Office**

If the **IP Stations**, **H.323 Trunks**, and **Remote Office** is set to `n`, the shuffling fields on the IP Network Regions screen do not display. You must enable these in the License File of the system.

Procedure

1. On the SAT screen, type **`change ip-network-region number`** and press `Enter`.

   The system displays the IP Network Region screen.

2. In **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** type one of the following:-

   - `y`: Permits shuffling the call.
   - `n`: Does not permit shuffling the call.
   - `native`: Uses the IP address of a telephone itself, or no translation by a Network Address Translation (NAT) device.
   - `translated`: Uses the translated IP address that a Network Address Translation (NAT) device provides for the native address.

   The **Intra-region IP-IP Direct Audio** field permits shuffling if both endpoints are in the same region. The **Inter-region IP-IP Direct Audio** field permits shuffling if the two endpoints are in two different regions.

   Note:

   If a NAT device is not in use, then the native and translated addresses are the same. For more information about NAT, see *Administering Avaya Aura® Communication Manager* and *Avaya Aura® Core Solution Description*.

3. On the Inter Network Region Connection Management screen, administer the common codec sets.

For more information about the fields on this screen, see *Avaya Aura® Communication Manager Screen Reference*.

Note:

You can connect IP endpoints in different network regions only when you enter the codec set to be used in the matrix. Also, you cannot share PROCR, Avaya Aura® Media Server, or G4xx Media Gateway resources among network regions.

Note:

Use any of the following commands for a list of codecs:

- `list ip-codec-set`
- `list ip-media-parameters`

4. Save the changes.

Related links

IP codec sets on page 78
Hairpinning and shuffling administration interdependencies on page 48

Codecs to administer and select

When an IP endpoint calls another IP endpoint, Communication Manager requests that the second endpoint choose the same codec that the first endpoint offered at call setup. However, if the second endpoint cannot match the codec of the first endpoint, the call is set up with the preferred codec for each endpoint. The data streams are converted between the endpoints, often resulting in degraded audio quality because of the different compressions or decompressions or multiple use of the same codec. For more information, see IP CODEC sets on page 78.

When a station or trunk initially connects to the server, Communication Manager selects the first codec that is common to both the server and the endpoint. The Inter Network Region Connection Management screen specifies the codec sets to use within an individual region (intra-region) and between or among (inter-region) network regions. If the endpoint and the G4xx Media Gateway or Avaya Aura® Media Server are in the same region, the administered intraregion codec set is chosen. If the endpoint and the G4xx Media Gateway or Avaya Aura® Media Server are in different regions, the administered inter-region codec set is chosen.

For example, a region might have its intranetwork codec administered as G.711 as the first choice, followed by other low bit rate codecs. The Inter Network Region Connection Management screen for the internetwork region might have G.729, a low-bit codec that preserves bandwidth, as the only choice. Initially, when a call is set up between these two interconnected regions, the G4xx Media Gateway or Avaya Aura® Media Server provides the audio stream conversion between G.711 and G.729. When the media stream is shuffled away from a TDM-based connection, the two endpoints can use only the G.729 codec.

Note:

For administering an H.323 trunk that uses Teletype for the Deaf (TTD), use the G.711 codec as the primary choice. This choice ensures accurate TTD tone transmission through the connection.

Administering H.323 trunks for shuffling

Before you begin

Ensure that you set the following fields on the Optional Features screen to `y`:

- **H.323 Trunks**
- **Remote Office**

If you set the **H.323 Trunks** and **Remote Office** field to `n`, the shuffling fields on the Signaling Group screen do not display. You must enable these features in the License File of the system.

Procedure

1. On the SAT screen, type **`change signaling group number`** and press `Enter`.

   The system displays the Signaling Group screen.

2. Set the **Direct IP-IP Audio Connections** field to `y`.

   After you set the **Direct IP-IP Audio Connections** field to `y`, shuffled IP calls use a public IP address by default.

3. Save the changes.

   Note:

   While administering an H.323 trunk that uses Teletype for the Deaf (TTD), use the G.711 codecs as the primary codec choice. This choice ensures accurate TTD tone transmission through the connection.

Related links

Hairpinning and shuffling administration interdependencies on page 48

Administering IP endpoints for shuffling

Before you begin

Ensure that the following fields on the Optional Features screen are set to `y`:

- **IP Stations** OR
- **Remote Office**

If the **IP Stations** or **Remote Office** fields are set to `n`, the hairpinning and shuffling fields on the Station screen do not display. These features must be enabled in the License File of the system.

About this task

Shuffling is independently administered for each endpoint on the Station screen. The specific station types that you can administer for shuffling are:

- All Avaya IP stations
- H.323-compatible stations from other vendors

Procedure

1. On the SAT screen, type **`change station extension`** and press `Enter`.

   The system displays the Station screen.

2. Set the **Direct IP-IP Audio Connections** field to `y`.

   After you set the **Direct IP-IP Audio Connections** field to `y`, shuffled IP calls use a public IP address by default.

3. Save the changes.

   Note:

   You cannot set the **Direct IP-IP Audio Connections** field to `y` if the **Service Link Mode** field is set to `permanent`.

Related links

Hairpinning and shuffling administration interdependencies on page 48

IP stations used for service observing in a call center

If a Call Center supervisor wants to service-observe an active shuffled call, the agent might notice a 200 ms break in the speech. The break occurs while the call is redirected to the TDM bus. To avoid the break in speech while the call is redirected, administer the shuffling and hairpinning fields as **n** (no) for stations that are used for service observing.

IP endpoint signal loss

The amount of loss applied between any two endpoints on a call is administrable. However, the Telecommunications Industry Association (TIA) has published standards for the levels that IP endpoints must use. The IP endpoints always send and receive audio at TIA standard levels. IP audio signals are sent or received over the TDM bus through a G4xx Media Gateway or Avaya Aura® Media Server. For these IP audio signals, the Media Module adjusts the levels to approximately match the levels of a signal to or from a DCP set. By default, IP endpoints are the same loss group as DCP sets, Group 2.

Loss to USA DCP levels

The switch instructs the G4xx Media Gateways or Avaya Aura® Media Server to insert loss into the signal coming from the IP telephone. The Media Module then inserts gain in the signal going to the IP telephone, to equal the levels of a signal to or from a DCP set.

The loss that is applied to a shuffled audio connection is constant for station-to-station, station-to-trunk, and trunk-to-trunk connection types.

Note:

The voice level on a shuffled call is not affected by entries administered in the 2-Party Loss Plan screen.

Fax, modem, TTY, H.323 Clear Channel calls over H.323 IP trunks, and SIP 64K Data calls over SIP trunks

Communication Manager uses the Relay mode or the Pass-through mode to transport fax, modem, and Teletypewriter device (TTY) calls over IP interfaces. Communication Manager supports transport of the following:

- TTY calls over the corporate Intranet and the Internet
- Faxes over a corporate Intranet or the Internet

  Note:

  Faxes sent to non-Avaya endpoints cannot be encrypted.
- T.38 fax over the Internet, including endpoints connected to non-Avaya systems
- Modem tones over the Internet, including endpoints connected to non-Avaya systems
- H.323 Clear Channel data calls over H.323 IP
- SIP 64K Data calls over SIP trunks
- Avaya devices are G430 and G450

Note:

Avaya no longer sells G250, G350, and G700.

Relay

In the Relay mode, the firmware on the device detects fax, modem, or TTY tones. To process the call over the IP network, the firmware uses the appropriate modulation protocol for fax or modem, or Baudot transport representation for TTY. The modulation and demodulation process for fax and modem calls reduces bandwidth use over the IP network as compared to the Pass-through mode. The Relay mode improves the reliability of transmission. The correct tones are regenerated before the calls reach the destination endpoint.

Note:

Do not use Avaya-proprietary fax and modem relay protocols. For modem relay applications, use the V.150.1 modem relay protocol. For fax relay applications, use the T.38 fax protocol.

Pass-through

In the Pass-through mode, the firmware on the device detects the tones of the call for fax, modem, or TTY. The firmware then uses G.711 encoding to carry the call over the IP network.

The Pass-through mode provides high-quality transmission when endpoints in the network are all synchronized to the same clock source.

Note:

The Pass-through mode increases the bandwidth use of each channel. However, you can make the same number of simultaneous fax or modem calls on the device as voice calls.

Note:

For the Pass-through mode on a modem and TTY calls over an IP network, the sending and receiving servers must have a common synchronization source. Using a source on the public network, you can establish synchronized clocks.

T.38

In the T.38 mode, the gateway DSP devices convert T.30 signals into T.38 packets and send the converted packets to a peer. If the fax endpoint on the far end supports T.30 signaling, the peer converts the packets back into T.30 signals and passes the packets to the fax endpoint. However, if the fax endpoint supports the T.38 protocol, the peer passes the packets directly to the fax endpoint.

T.38 is the preferred industry standard fax protocol. H.323 and SIP trunks support the T.38 protocol.

Communication Manager uses the T.38 protocol for fax transmission over IP network facilities. 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.

For more information about FAX over IP and T.38-G711-fallback, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

V.150.1 Modem Relay

The V.150.1 protocol is an ITU-T recommendation for the transmission of modem data over IP networks. This protocol is the preferred industry-standard modem relay protocol. SIP trunks support the V.150.1 Modem Relay mode. In the V.150.1 Modem Relay mode, modem features are implemented according to ITU-T V-series recommendations. These recommendations are used for interoperation with the non-Avaya trunk-side and line-side modem equipments, and with native-V.150.1 secure IP endpoints. This mode uses the V.150.1 protocol that defines how to send modem traffic between modems and telephone devices over an IP network. This mode also supports Modem-over-IP interoperability with SIP endpoints and third-party SIP gateways. This mode uses the Simple Packet Relay Transport (SPRT) protocol to send data between V.150.1–capable endpoints.

SIP 64K Data

With SIP 64K Data, Communication Manager controls the mechanism to enable the support of the RFC 4040 media service.

Communication Manager uses RFC 4040 Clear Mode data transport to support the media transport of ISDN traffic. The ISDN traffic is directed to a destination that is reached through a SIP trunk.

Associated with the **SIP 64K Data** field are two other fields, **Redundancy** and **Packet Size (ms)**. Communication Manager communicates the values of the **Redundancy** and **Packet Size (ms)** fields to the media gateway so that the gateway properly operates with the DSP conversion of the TDM media into an IP media stream.

For more information about **Redundancy** and **Packet Size (ms)** fields, see *Avaya Aura® Communication Manager Screen Reference*.

Administering fax, TTY, modem, and clear-channel calls over IP trunks

About this task

Using ISDN-PRI trunks, calls are sent either over the public network or over an H.323 or SIP private network to Communication Manager switches.

The endpoints that send and receive the calls must be connected to a private network. The private network uses H.323, SIP, or LAN connections between gateways or port networks.

Procedure

1. Create one or more IP codec sets that enable the appropriate transmission modes for the endpoints on gateways.

   Note:

   Create the fax, modem, TTY, and clear-channel settings, including redundancy, on the second page of the IP Media Parameters screen.

2. Assign each codec set to the appropriate network region.
3. Assign the network region to the appropriate devices:
   - G4xx Media Gateway or Avaya Aura® Media Server
   - Avaya G430 or G450 branch gateways
4. **(Optional)** Administer internetwork region connections if the G4xx Media Gateway or Avaya Aura® Media Server are shared among administered network regions.

Related links

Defining IP interfaces on page 28
IP codec sets on page 78
IP network regions on page 81
Manually interconnecting the network regions on page 101

Considerations for administering FAX, TTY, modem, and Clear-Channel transmission

When configuring your system for FAX, TTY, modem, and Clear-Channel calls over an IP network, consider the following factors:

- Encryption

  You can encrypt most types of relay and pass-through calls using the Avaya Encryption Algorithm (AEA) or the Advanced Encryption Standard (AES). See Media encryption for FAX, modem, TTY, and clear channel on page 68.

- Bandwidth usage

  Bandwidth use of modem relay varies, depending on the packet size used and the redundancy level selected. The packet size for modem relay is determined by the packet size of the codec selected. Bandwidth use of modem pass-through varies depending on the redundancy level and packet size selected. The maximum packet size for modem pass-through is 20 ms.

  Bandwidth use for other modes also varies, depending on the packet size used, whether redundant packets are sent and whether the relay or pass-through method is used.

  For the bandwidth usage, see Table 4: Bandwidth for FAX, modem, and TTY calls over IP networks on page 67 .

- Calls with non-Avaya systems

  Some FAX calls might have one communicating endpoint connected to a non-Avaya communications system. For such FAX calls, the non-Avaya system and the Avaya system must both have T.38 defined for the codecs.

  Modem and TTY calls over the IP network cannot be successfully sent to non-Avaya systems. Modem V.150.1 calls are interoperable with other systems that also support the V.150.1 protocol.

- Differing transmission methods at the sending or receiving endpoints

  The transmission method or methods used on both the sending and receiving ends of a FAX/modem/TTY/clear channel call must be the same.

  Sometimes, a call succeeds although the transmission method for the sending and receiving endpoints is different. Usually, for a call to succeed, the two endpoints must be administered for the same transmission method.

- H.320 Video over IP using Clear Channel

  H.320 Video over IP using Clear Channel is supported. To support H.320 Video over IP, the port networks or the gateways must have reliable Synchronization Sources and transport for framing integrity of the channels.

- Hardware requirements

The relay and pass-through capabilities require the following hardware:

- For Avaya S8300E Servers, G450, G430 Branch Gateway, and the Multi-Tech MultiVoIP Gateway, the firmware must be updated to the latest available on http://support.avaya.com
- For T.38 FAX capability, endpoints on other non-Avaya T.38 compliant communications systems can send or receive FAX calls using endpoints on Avaya systems.

- Multiple hops and multiple conversions

A FAX call can undergo two or more conversion cycles, from TDM protocol to IP protocol and back to TDM protocol. In such situations, the call can fail because of delays in processing through more than one conversion cycle. A modem or TTY call can undergo only one conversion cycle, from TDM to IP protocol and back to TDM protocol, on the communication path. If multiple conversion cycles occur, the call fails. Therefore, both endpoint gateways and any intermediate servers in a path containing multiple hops must support shuffling for a modem or TTY call to succeed.

For example, in the following figure, a hop occurs in either direction for calls between port network A and Gateway C. The calls are transcoded between point B and point D. In this case, shuffling is required on devices A, B, C, and D.

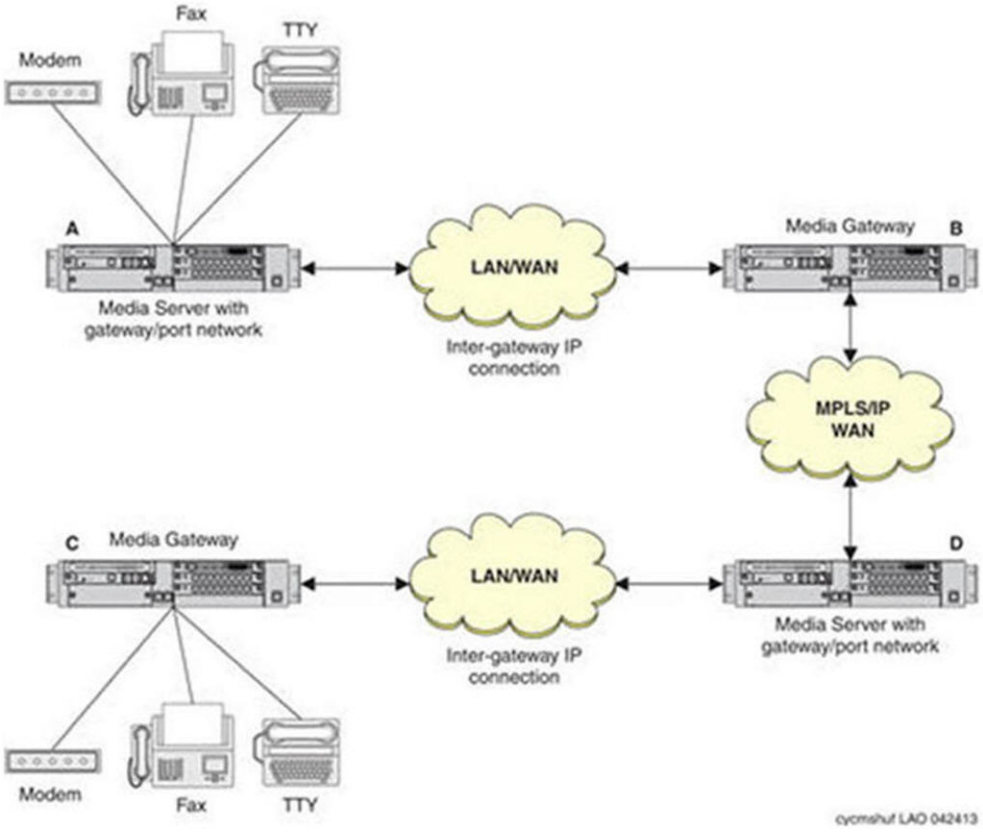


Figure 8: Shuffling for FAX, modem, and TTY calls over IP

FAX, TTY, modem, and clear channel transmission modes and speeds

Communication Manager provides many methods for supporting FAX, TTY, modem, and clear channel transmission over IP.

Note:

FAX Relay, FAX Pass-through, TTY Pass-through, Modem Relay, and Modem Pass-through are proprietary solutions that work only between two Avaya-supported endpoints, such as media gateways and Communication Manager port networks.

Table 3: FAX, TTY, modem, and clear channel transmission modes and speeds

Mode	Maximum rate	Comments
T.38 FAX Standard (relay only)	9600 bps	This capability is standards-based and uses IP trunks, H.323 or SIP for communicating with non-Avaya systems. Additionally, the T.38 FAX capability uses the User Datagram Protocol (UDP). For more information, see T.38 fax standard mode. **Note:** FAX endpoints served by two different Avaya servers can also send T.38 faxes to each other if both systems are enabled for T.38 FAX. In this case, the servers also use IP trunks.
FAX Relay	9600 bps	Because the data packets for faxes in relay mode are sent almost exclusively in one direction, from the sending endpoint to the receiving endpoint, bandwidth use is reduced. **Note:** Do not use this proprietary relay protocol. Instead, use T.38 FAX standard or T.38 with fallback to G.711 Pass-through.

Table continues…

Mode	Maximum rate	Comments
FAX Pass-through	V.34 (33.6 kbps)	The transport speed is up to the equivalent of circuit-switched calls and supports G3 and Super G3 FAX rates. **Note:** You can achieve the V.34 speed of 33.6 Kbps if the IP transport network has minimum delay and only a few hops. If you are using Super G3 FAX machines as well as modems, do not assign these FAX machines to a network region with an IP Codec set that is modem-enabled as well as FAX-enabled. If its Codec set is enabled for both modem and FAX signaling, a Super G3 FAX machine incorrectly tries to use the modem transmission instead of the FAX transmission. Therefore, assign modem endpoints to a network region that uses a modem-enabled IP Codec set and assign the Super G3 FAX machines to a network region that uses a FAX-enabled IP Codec set. You can assign packet redundancy in both Pass-through and Relay modes, which means that the gateways use packet redundancy to improve packet delivery and robustness of FAX transport over the network. The Pass-through mode uses more network bandwidth than the Relay mode. Redundancy increases bandwidth usage even more.
T.38 with fallback to G.711 Pass-through	9600 bps	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. This mode requires a G.711 codec to be administered on the IP Media Parameters screen. **Note:** The T.38 with fallback to G.711 Pass-through feature only works over SIP trunks.
TTY Relay	16 kbps	This transport of TTY supports US English TTY (Baudot 45.45) and UK English TTY (Baudot 50). TTY uses RFC 2833 or RFC 2198 style packets to transport TTY characters. Depending on the presence of TTY characters on a call, the transmission toggles between voice mode and TTY mode. The system uses up to 16 Kbps of bandwidth, including packet redundancy, when sending TTY characters and normal bandwidth of the audio codec for the voice mode.

Table continues…

Mode	Maximum rate	Comments
TTY Pass-through	87-110 kbps	In the Pass-through mode, you can also assign packet redundancy, which means that the gateways send duplicated TTY packets to ensure and improve quality over the network. The pass-through mode uses more network bandwidth than the relay mode. Pass-through TTY uses 87-110 kbps, depending on the packet size, whereas TTY relay uses, at most, the bandwidth of the configured audio codec. Redundancy increases bandwidth usage even more.
Modem Relay	V.32 (9600 bps)	The maximum transmission rate can vary with the version of firmware. The packet size for modem relay is determined by the packet size of the codec selected but is always at least 30 ms. Also, each level of packet redundancy, if selected, increases the linear bandwidth usage . The first level of redundancy doubles the bandwidth usage, the second level of redundancy triples the bandwidth usage, and so on. **Note:** Modem over IP in relay mode is currently available only for use by specific secure analog telephones that meet the Future Narrowband Digital Terminal (FNBDT) standard. Do not use this proprietary relay protocol. Instead, use the V.150.1 standard-based relay protocol.
Modem Pass-through	V.34 (33.6 kbps) and V.90/V.92 (43.4 kbps)	Transport speed depends on the negotiated rate of the modem endpoints. Though the servers and gateways support modem signaling at v.34 (33.6 kbps) or v.90 and v.92 (43.4 kbps), the modem endpoints can automatically reduce transmission speed to ensure maximum quality of signals. V.90 and V.92 are speeds typically supported by modem endpoints only when directly connected to a service provider Internet service. You can also assign packet redundancy in pass-through mode, which means that the gateways send duplicated modem packets to improve packet delivery and robustness of FAX transport over the network. Pass-through mode uses more network bandwidth than relay mode. Redundancy increases bandwidth usage even more. The maximum packet size for modem pass-through is 20 ms.
Clear-Channel	64 kbps (unrestricted)	The Clear-Channel mode supports only clear channel data, but not analog data transmission functionality such as FAX, modem, TTY, or DTMF signals. The Clear-Channel mode is purely a clear channel data. In addition, support is unavailable for echo cancellation, silence suppression, or conferencing. H.320 video over IP using clear channel is supported if the port networks or the gateways have a reliable synchronization source and transport for framing integrity.

Table continues…

Mode	Maximum rate	Comments
V.150.1 Standard Modem Relay	Need information	V.150.1 protocol is standards-based and uses SIP signaling for communication with non-Avaya systems. This protocol uses one RTP port for sending RFC 2833 tone events, a second RTP port for exchanging State Signaling Events (SSE), and a third RTP port for sending the Simple Packet Relay Transport (SPRT) data packets. The sending and receiving systems negotiate for the support of V.150.1 in the SDP message set of the SIP protocol. The two principle applications are: • Commercial telemetry data transport • Secure SIP station set voice transport

T.38 fax standard mode

H.323 and SIP call transport segments can be deployed for a single call path. Each time the call traverses from one technology to the other, a pair of transcoding is generated. H.323 and SIP in a fax call path can work if one of the end devices is a fax server that integrates using IP. Keep the number of transcoding nodes to three or fewer to keep the delay to an acceptable level.

The T.38 FAX sending and receiving endpoints can be on port networks or gateways registered to the same server. In such cases, the gateways or port networks revert to Avaya FAX relay mode.

The sending and receiving systems must announce the support of T.38 FAX data applications. Support for T.38 FAX data applications must be announced during the H.245 capabilities exchange for H.323 trunks or the SDP media description for SIP trunks. Avaya systems announce support of T.38 FAX if the capability is administered on the Codec Set screen for the region. Also, a T.38-capable media processor must be chosen for the voice channel. In addition, for a successful FAX transmission, both systems must support the H.245 null capability exchange to avoid multiple IP hops in the connection.

Note:

To use the T.38 FAX capability, disable modem Relay and modem Pass-through. However, the modem Pass-through mode can use the T.38 FAX capability even if the mode is not disabled. Additionally, the T.38 FAX capability does not support TCP.

If you experience a packet network loss, assign packet redundancy to T.38 standard faxes to improve packet delivery and robustness of FAX transport over the network.

T.38 FAX Standard supports Error Correction Mode (ECM). With ECM, a FAX page is transmitted in a series of blocks that contain frames with packets of data.

After receiving the data for a complete page, a receiving fax machine notifies the transmitting fax machine of any frames with errors. The transmitting fax machine then retransmits the specified frames. This process is repeated until all frames are received without errors. If the receiving fax machine is unable to receive an error-free page, the fax transmission can fail and one of the fax machines can disconnect. too much content for a table. Create a separate concept topic and link.

Bandwidth for FAX, modem, TTY, and clear channel calls over IP networks

The following table identifies the bandwidth of FAX, modem, TTY, and clear channel calls based on the following factors:

- Packet sizes
- Redundancy
- Relay or Pass-Through method

The values are approximate because bandwidth can vary during each call for multiple reasons.

Table 4: Bandwidth for FAX, modem, and TTY calls over IP networks

Packet Size (in msec)	Bandwidth (in kbps) (bidirectional)									
	Redundancy = 0						Redundancy = 1		Red. = 2	Red. = 3
	TTY at G.711	TTY at G.729	TTY at G.723	FAX Relay	Modem Relay at 9600 Baud	Clear Channel FAX/ Modem pass-through	FAX Relay	Clear Channel FAX/ Modem pass-through	FAX Relay [3] [4]	FAX Relay[3] [4]
10	110	54	-	-	-	110	-	221	-	-
20	87	31	-	-	-	87	-	174	-	-
30	79	23	22	25	22.9	-	50	-	75	100
40	76	20	-	-	19.6	-	-	-	-	-
50	73	17	-	-	17.6	-	-	-	-	-
60	72	16	14	-	16.3	-	-	-	-	-

TTY, Modem Relay, Modem pass-through, and FAX pass-through calls are full duplex. Multiply the bandwidth of the mode by 2 to get the network bandwidth usage.

TTY at G723 supports 30 and 60 ms packet size.

FAX Relay supports 30 ms packet size.

Nonzero redundancy options increase the bandwidth usage by a linear factor of the bandwidth usage when the redundancy is zero.

FAX and Modem pass-through support 10 and 20 ms packet size.

Clear Channel transport supports a packet size of 20 ms.

Media encryption for FAX, modem, TTY, and clear channel

If media encryption is configured, the algorithm used during the audio channel setup of the call is maintained for most FAX relay and pass-through modes. The exception is the T.38 standard for FAX over IP, for which encryption is not used.

Encryption is applicable as shown in the following table.

Table 5: Encryption options

Call Type	AEA	AES	SRTP	Transport
Modem Pass-through	Y	Y	Y	RTP (RFC2198)
Modem Relay	Y	N	N	Proprietary
V.150.1 Modem Relay	N	N	N	Simple Packet Relay Transport (SPRT)
FAX Pass-through	Y	Y	Y	RTP (RFC2198)
FAX Relay	Y	N	N	Duplicate Packets
TTY Pass-through	Y	Y	Y	RTP (RFC2198)
TTY Relay	Y	Y	Y	RFC2198
T.38 FAX Standard	N	N	N	T.38 UDPTL Redundancy
Clear Channel	Y	Y	Y	RTP (RFC2198)

Note:

For more information about the SRTP encryption protocol, see SRTP media encryption on page 69.

If the audio channel is encrypted, the FAX digital channel is also encrypted, except for the limitations described above. AEA-encrypted FAX and modem relay calls that switch back to audio continue to be encrypted using the same key information used at audio call setup.

For the cases of encrypting FAX, modem, and TTY pass-through and TTY relay, the encryption used during audio channel setup is maintained during the call.

The software works in the following way for encryption:

- For FAX, modem, and TTY pass-through and relay, VoIP firmware encrypts calls as administered on the CODEC set screen. These calls begin in voice, so VoIP encrypts the voice channel as administered. If the media stream is converted to FAX, modem, or TTY digital, the VoIP firmware automatically disables encryption as appropriate. When the call switches back to audio, VoIP firmware encrypts the stream again.
- For T.38 FAX, VoIP firmware encrypts the voice channel as administered on the CODEC set screen. When the call is converted to FAX, VoIP firmware automatically turns off encryption. If the call later reverts back to audio, VoIP firmware encrypts the stream again.

Setting network performance thresholds

About this task

You require a craft login or a higher login to perform this administration.

Communication Manager provides control over four IP media packet performance thresholds to streamline VoIP traffic. You can use the default values for these parameters, or you can change the values to fit the needs of your network. These threshold values apply only to IP trunks and do not affect other IP endpoints.

Procedure

1. On the SAT screen, type `change signaling-group` *n*.
2. On the Signaling Group screen, in the Group Type field, type `h.323` or `sip`.
3. In the **Bypass If IP Threshold Exceeded** field, type `y`.

   If bypass is activated for a signaling group, the system compares the ongoing measurements of network activity with the values in the IP-options system-parameters screen. If the current measurements exceed the values in the IP-options system-parameters screen, the bypass function terminates use of the network path for the signaling group. The following actions are taken when thresholds are exceeded:

   - Existing calls on the IP trunk associated with the signaling group are not maintained.
   - Incoming calls do not arrive at the IP trunks on the bypassed signaling group and are diverted to alternate routes.
   - Outgoing calls are blocked on this signaling group.

     If so administered, blocked calls are diverted to alternate routes, either IP or circuits, as determined by the administered routing patterns.

     Note:

     Use the default values.

SRTP media encryption

Secure Real Time Protocol (SRTP) is a media encryption standard that provides encryption of RTP media streams for SIP and 9600-series IP telephones. SRTP is defined in RFC 3711.

The following SRTP features are supported by Communication Manager Release 4.0 and later:

- Encryption of RTP. Encryption is optional, but recommended.
- Authentication of RTCP streams. Authentication of RTCP streams is mandatory.
- Authentication of RTP streams. Authentication of RTP streams is optional, but recommended.
- Protection against replay.

The following SRTP features are not supported by Communication Manager:

- Several automatic rekeying schemes
- Other options within SRTP that are not expected to be used for VoIP, such as key derivation rates or MKIs

Previous releases of Communication Manager supported AEA and AES media encryption for H.323 calls, however no media encryption was available for SIP calls. Starting with Release 4.0, SRTP provides encryption and authentication of RTP streams for SIP. SRTP also provides authentication of RTP and RTCP for SIP and H.323 calls using the 9600-series telephones.

SRTP encryption of FAX and modem relay and T.38 is not supported. FAX and modem relay and T.38 are not transmitted in RTP. Therefore, where an SRTP voice call changes to a fax relay, fax is not encrypted.

SRTP is available only if :

- Media Encryption is enabled in the license file.
- Media Encryption is activated by IP codec set administration in the same manner as for other encryption algorithms.

In Communication Manager Release 7.0 and later, you can 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.

Also, in Communication Manager Release 7.0 and later, the AES encryption option now includes AES-256. AES-256 applies to voice media streams and video media streams for the IP network region that governs the ip-codec-set

Platforms

The SRTP feature is supported on all Linux-based platforms running Communication Manager. The SRTP feature is also supported on all versions of SES, regardless of platform, starting with Release 4.0.

The following gateway platforms also support SRTP, SRTCP, and AES-256:

- Avaya Aura® Media Server
- VoIP Media Modules and on-board VoIP engines as follows:
  - G430 Branch Gateway
  - G450 Branch Gateway

Administering SRTP

Before you begin

Ensure that the Media Encryption over IP feature is enabled in the license file.

About this task

Administering SRTP encryption is the same as administering AES and AEA encryption.

Procedure

1. On the Customer Options form, ensure that the **Media Encryption Over IP?** field is set to `y`.
2. On the IP Media Parameters form, administer the Media Encryption type in the **Media Encryption** field.

   You can use this field to specify a priority listing for one of five available options for the negotiation of encryption.

   For two network regions that have different codec sets that are assigned to a third codec set. The settings for media Encryption will then depend on the third codec set.
3. Administer the ip-network-region form for SIP options.

   Use the **Allow SIP URI Conversion?** field to specify whether a SIP Uniform Resource Identifier (URI) is permitted to change. For example, if sips:// in the URI is changed to sip://, then the call can be less secure. However, changing to a less secure URI can be necessary to complete the call. In the **Allow SIP URI Conversion?** field, you can enter `n` to forbid URI conversion. Then calls made from SIP endpoints that support SRTP to other SIP endpoints that do not support SRTP fail. Enter `y` for converting SIP URIs. The default is `y`.
4. Configure an endpoint to use SRTP.

   For an endpoint, set SRTP as media encryption and TLS as transport.

   To enable the SRTP on an endpoint:

   - Use 46xxSettings.txt to set MEDIAENCRYPTION 10, 11 (Support 10-srtp-aescm256-hmac80, 11-srtp-aescm256-hmac32 if you want to use AES-256 media encryption)
   - Use 46xxSettings.txt to set MEDIAENCRYPTION 1, 9 (Support 1-srtp-aescm128-hmac80, 9=none as recommended)
   - Use 46xxSettings.txt to set SIPSIGNAL 2 (2 to use Transport protocol as TLS)

   For more information about administering SRTP, see *Media Encryption*

Administering SRTP for video signaling

Procedure

1. Type `change system-parameters customer-options`.

   The system displays the Optional Features screen.

2. On page 4 of the Optional Features screen, set the **Media Encryption Over IP** field to `y`.

   This setting applies both audio and video SRTP.

3. Type `change system-parameters features`.

   The system displays the Feature-Related System Parameters screen.

4. On page 19 of the Feature-related System Parameters screen, set the **Initial INVITE with SDP for secure calls** field to `y`.

5. Type `change signaling-group n`, where *n* is the signaling group number.

   The system displays the Signaling Group screen.

6. Set the **Enforce SIPS URI for SRTP** field to `y`.

7. Type `change system-parameters ip-options`.

   The system displays the IP-Options Systems Parameters screen.

8. On page 2 of the IP-Options Systems Parameters screen, set the **Override ip-codec-set for SIP direct-media connections** field to:

   - `n` if you are running Communication Manager 6.3.2 or later.
   - `y` if you are running an earlier release of Communication Manager.

9. Type any of the following:

   - `change ip-codec-set n`
   - `change ip-media-parameters n`

   Where *n* is the ip codec set number.

   The system displays the IP Media Parameters screen.

10. In the **Media Encryption** section, administer the SRTP options.

    a. In field 1, type `10-srtp-aescm256-hmac80`.

    b. In field 2, type `11-srtp-aescm256-hmac32`.

    c. In field 3, type `1-srtp-aescm128-hmac80`.

    d. In field 4, type `2-srtp-aescm128-hmac32`.

    e. In field 5, type `none`.

    Note:

    For video calls to work on the Best Effort SRTP mode, select **none**.

11. Repeat Step 6 for each ip codec set.

Chapter 4: Voice, Video, and Network quality administration

This chapter provides information about:

- Improving voice quality by adjusting the voice packet traffic flow through an IP network, also known as implementing Quality of Service (QoS).
- Network recovery and survivability

Note:

Implementing QoS requires administration adjustments to Avaya equipment as well as LAN/WAN equipment, such as switches, routers, and hubs.

For more information about QoS, see *Avaya Aura® Core Solution Description*.

For more information about implementing QoS, see the White Paper, *Avaya IP Voice Quality Network Requirements (LB1500-02)*, at http://www.support.avaya.com.

Factors causing voice degradation

VoIP applications put severe constraints on the amount of end-to-end transfer delay of voice signal and routing. If these constraints are not met, users complain of garbled or degraded voice quality, gaps, and pops. Due to human voice perception, VoIP applications can afford to randomly lose a few voice packets and the user can still understand the conversation. However, if voice packets are delayed or systematically lost, the destination experiences a momentary loss of sound, often with some unpleasing artifacts like clicks or pops. Some general complaints and their causes are listed in the following table:

Table 6: User complaints and their causes

Complaint	Possible causes and links to information
'Talking over' the far end	• Packet delay and loss • Echo • Network architecture between endpoint and intermediate node • Switching algorithms
Echo at the near-end and far-end	• Impedance mismatch • Improper coupling • Codec administration
Too soft or too loud voice	• PSTN loss • Digital loss • Automatic Gain Control • Conference loss plan
Clicks, pops, or stutters	• Packet loss • Timing drift due to clocks • Jitter • False DTMF detection • Silence suppression algorithms
Muffled, distorted, or noisy sound	• Codec administration • Transducers • Housings • Environment • Analog design

Some factors causing voice degradation are:

- Packet delay and loss
- Echo
- Transcoding

Packet delay and loss

The causes of voice degradation include:

- Packet delay or latency

  The following factors can cause packet delay or latency:

  - Buffer delays

- Queuing delays in switches and routers
- Bandwidth restrictions

- Jitter or statistical average variance in end-to-end packet travel times
- Packet loss

  The following factors can cause packet loss:

  - Network overload
  - Full jitter buffers
  - Echo

Tip:

Use a network assessment that measures and solves latency issues before implementing VoIP solutions. For more information, see *Avaya Aura® Core Solution Description*.

Transcoding

When IP endpoints are connected through more than one network region, each region must use the same codec. A codec is the circuitry that converts an audio signal into the digital equivalent and assigns companding properties. Packet delays occur when different codecs are used within the same network region. In this case, the G4xx Media Gateway or Avaya Aura® Media Server acts as a gateway translating the different codecs, and an IP-direct or shuffled connection is not possible.

Bandwidth

In converged networks that contain coexistent voice and data traffic, the volume of either type of traffic is unpredictable. For example, transferring a file using the File Transfer Protocol (FTP) can cause a sharp burst in the network traffic. At other times, the network might have no data.

While most data applications are insensitive to small delays, the recovery of lost and corrupted voice packets is a significant problem. For example, users are not concerned if the reception of email or files from file transfer applications is delayed by a few seconds. In a voice call, the most important expectation is the real-time exchange of speech. To achieve real-time communication, network resources are required for the complete duration of the call. If resources are unavailable or the network is too busy to carry the voice packets, clicks, pops, and stutters are heard at the destination. Therefore, for real-time exchange of speech with adequate quality, a fixed amount of bandwidth is continually required during the call.

Quality of Service and voice quality administration

Delay is a crucial cause of VoIP quality degradation, and many other causes are highly interdependent with delay. Therefore, delay must be reduced by improving the routing in the network or by reducing the processing time within the endpoints and intermediate nodes.

For example, when delay is minimized:

- Jitter and electrically induced echo abate.
- Intermediate node and jitter buffer resources are released making packet loss insignificant.

  As packets move faster in the network, the resources at each node are available for the next packet that arrives. Packets are not dropped because of lack of resources.

Delay cannot be eliminated completely from VoIP applications because delay includes the inevitable processing time at the endpoints plus the transmission time. However, the delay that is caused because of network congestion or queuing can be minimized by adjusting the following Quality of Service (QoS) parameters:

- Layer 3 QoS
  - DiffServ
  - RSVP
- Layer 2 QoS: 802.1p/Q

These parameters are administered on the IP Network Region screen. See IP network regions.

Layer 3 QoS

DiffServ

The Differentiated Services Code Point (DSCP) or DiffServ is a packet prioritization scheme. DiffServ uses the Type of Service (ToS) byte in the packet header to indicate the forwarding class of the packet and Per Hop Behaviors (PHBs). After the packets are marked with the forwarding class, the interior routers and gateways use this ToS byte to differentiate the treatment of packets.

A DiffServ policy must be established across the entire IP network. The DiffServ values used by Communication Manager and by the IP network infrastructure must be the same.

If you have a Service Level Agreement (SLA) with a service provider, the volume of traffic of each class that you can inject into the network is limited by the SLA. The forwarding class is directly encoded as bits in the packet header. After the packets are marked with the forwarding class, the interior nodes, including routers and gateways, can use this information to differentiate treatment of packets.

RSVP

Resources Reservation Protocol (RSVP) can be used to lower DiffServ priorities of calls when bandwidth is scarce. The RSVP signaling protocol sends requests for resource reservations to routers on the path between the sender and the receiver for the voice bearer packets. RSVP does not send requests for resource reservation for call setup or call signaling packets.

Layer 2 QoS

802.1p is an Ethernet tagging mechanism that can process Ethernet switches to give priority to voice packets.

Caution:

If you change 802.1p/Q on the IP Network Region screen, the format of the Ethernet frames changes. 802.1p/Q settings in Communication Manager must match similar settings in your network elements.

The 802.1p feature is important to the endpoint side of the network because personal computer-based endpoints must rank audio traffic over routine data traffic.

For IEEE standard 802.1Q, you must specify both a virtual LAN (VLAN) and a frame priority at layer 2 for LAN switches or Ethernet switches, for routing based on MAC addresses.

802.1p/Q provides 8 priority levels and many Virtual LAN identifiers. Interpretation of the priority is controlled by the Ethernet switch and is usually based on highest priority first. The VLAN identifier permits segregation of traffic within Ethernet switches to reduce traffic on each link. 802.1p operates on the MAC layer. The switch always sends the QoS parameter values to the IP endpoints. Attempts to change the settings by DHCP or manually are overwritten. The IP endpoints do not process the VLAN on or off options. Turning VLAN on requires that the capabilities be administered on the LAN switch nearest to the IP endpoint. VLAN tagging can be turned on manually, by DHCP, or by TFTP.

If you have varied 802.1p from LAN segment to LAN segment, then you must administer 802.1p/Q options individually for each network interface. You require a separate network region for each network interface.

VLANs

Virtual Local Area Networks (VLANs) provide security and create smaller broadcast domains by using software to create virtually separated subnets. The broadcast traffic from a node that is in a VLAN goes to all nodes that are members of the VLAN. Thus, VLANs reduce CPU use and increase security by restricting the traffic to a few nodes, instead of every node on the LAN.

Any end-system that performs VLAN functions and protocols is VLAN-aware. However, very few end-systems are VLAN-aware. VLAN-unaware switches cannot handle VLAN packets from VLAN-aware switches. Hence, Avaya gateways have VLAN configuration turned off by default. Create separate VLANs for VoIP applications.

Administering endpoints for IP address mapping

Procedure

1. On the SAT screen, type `change ip-network-map` and press `Enter`.

   The system displays the IP Address Mapping screen.

2. In the **FROM IP Address** field, type the starting IP address.

   You can type IPv4 or IPv6 address.

   The IPv4 address must be a 32-bit address with four decimal numbers, each in the range 0-255 and IPv6 address must be 128–bit address with Hexadecimal numbers.

3. In the **TO IP Address** field, type the terminating IP address.

You can type IPv4 or IPv6 address.

The IPv4 address must be a 32-bit address with four decimal numbers, each in the range 0-255 and IPv6 address must be 128–bit address with Hexadecimal numbers.

If the **TO IP Address** field and the **Subnet Mask** field are blank , the address in the **FROM IP Address** field is copied into this field.

4. In the **or Subnet Mask** field, specify the mask to be used to get the subnet work identifier from the IP address.

   If this field is nonblank on submission, then:

   - Mask is applied to the **FROM IP Address** field, putting zeros in the non-masked rightmost bits. The address becomes the stored From address.
   - Mask is applied to the **TO IP Address** field, putting 1s in the non-masked rightmost bits. This address becomes the stored To address.

     Valid entries are a number in the range 0-32 or blank.

   The **Subnet Mask** field and the **TO IP Address** field can be submitted blank. When both the fields are blank, the address in the **FROM IP Address** field is copied into the **TO IP Address** field

5. In the **Region** field, type the network region for the IP address range.

   The **Region** field must contain the network region for this interface. The value can be a number in the range 1-250.

6. In the **VLAN** field, specify the virtual LAN value.

   The **VLAN** field sends the VLAN instructions to IP endpoints such as IP telephones and IP softphones. This field does not send instructions to the PROCR.

   The **VLAN** field can take a value between 0-4095 if you want to specify the virtual LAN value. Set the **VLAN** field to n to indicate that VLAN is disabled.

7. In the **Emergency Location Extension** field, type a value 1-7 digits long for the emergency location extension.

   The default value is blank. A blank entry is often used for an IP softphone dialing in through PPP from outside your network.

   The entry on this screen can be different from the value entered in the **Emergency Location Extension** field on the Station screen. When such a mismatch occurs, the extension entered on this screen is sent to the Public Safety Answering Point (PSAP).

8. Save the changes.

IP codec sets

The type of codec used for voice encoding and companding, and compression or decompression are available on the IP Media Parameters screen. The codecs on the IP Media Parameters screen are listed in the order of preferred use. A call across a trunk between two systems is set up to use the first common codec listed.

Note:

The codec order must be administered the same for each system of an H.323 trunk connection. The set of codecs listed does not have to be the same, but the order of the listed codecs must.

In the IP Media Parameters screen, define the codecs and packet sizes used by each IP network region. You can also enable or disable silence suppression for each codec in the set. The screen dynamically displays the packet size in milliseconds (ms) for each codec in the set, based on the number of 10 ms frames that you administer for each packet.

Finally, you use this screen to assign the following characteristics to a codec set:

- Whether endpoints in the assigned network region can route FAX, modem, TTY, or clear channel calls over IP trunks.
- The mode that the system uses to route the FAX, modem, TTY, or clear channel calls.
- Whether redundant packets must be added to the transmission for higher reliability and quality.

Note:

For pass-through mode, payload redundancy per RFC2198 is used.

These characteristics must be assigned to the codec set, and the codec set must be assigned to a network region. Only after assigning are the endpoints in that region able to use the capabilities established on this screen.

Caution:

Users might use Super G3 FAX machines and modems. Do not assign these FAX machines to a network region with an IP Codec set that is both modem-enabled and FAX-enabled. Do not enable the codec set for both modem and FAX signaling. If both are enabled, a Super G3 FAX machine incorrectly tries to use the modem transmission instead of the FAX transmission. Therefore, assign modem endpoints to a network region that uses a modem-enabled IP Codec set. Assign the Super G3 FAX machines to a network region that uses a FAX-enabled IP Codec set.

Related links

Administering shuffling in network regions on page 54

Administering an IP Codec set

Procedure

1. Type any of the following and press `Enter`:
   - `change ip-codec-set` *n*
   - `change ip-media-parameters` *n*

   The system displays the IP Media Parameters screen.
2. In the **Audio Codec** field, specify an audio CODEC.

3. In the **Silence Suppression** field, perform one of the following tasks:
   - If you want to avoid silence suppression, type `n`.
   - If you require silence suppression on the audio stream, type `y`.

   Silence suppression can affect audio quality.
4. In the **Frames per Pkt** field, specify frames for each packet.

   The frame value can be between 1 to 6.

   The system displays the **Packet Size (ms)** field automatically.
5. In the **Media Encryption** field, specify an option for the negotiation of encryption.

   The system displays this field only if the Media Encryption over IP feature is enabled. The system specifies one of the five possible options for the negotiation of encryption. The selected option for an IP codec set applies to all codecs defined in that set.
6. Go to page 2 of the screen.

   Note:

   Use these approximate bandwidth requirements to decide which codecs to administer. These numbers change with packet size and include layer 2 overhead. With 20 ms packets, the following bandwidth is required:

   - 711 A-law–85 kbps
   - 711 mu-law–85 kbps, used in the U.S. and Japan
   - 729–30 kbps
   - 729A/B/AB–30 kbps audio
   - OPUS Codec bit-rate options:
     - OPUS-NB12K : 12 kbps
     - OPUS-NB16K : 16 kbps
     - OPUS-WB20K: 20 kbps
     - OPUS-SWB24: 24 kbps
7. In the **All Direct-IP Multimedia?** field, type `y` for direct multimedia through the following codecs:
   - H.261
   - H.263
   - H.264 (video)
   - H.224
   - H.224.1 (data, far end camera control)

8. In the **Maximum Bandwidth Per Call for Direct-IP Multimedia** field, enter the unit of measure corresponding to the numeric value entered for the bandwidth limitation. The unit of measure can be kbits or mbits.

   The system displays this field only when **Allow Direct-IP Multimedia** is `y`.

9. In the **FAX Mode** field, specify the mode for fax calls.
10. In the **Modem Mode** field, specify the mode for modem calls.
11. In the **TDD/TTY Mode** field, specify the mode for TDD/TTY calls.
12. In the **Clear Channel** field, type `y or n`.
    - If the value is `y`, 64 kbps clear channel data calls is possible for this codec set.
    - If the value is `n`, 64 kbps clear channel data calls is not possible for this codec set.
13. In the **Redundancy** field, perform one of the following:
    - For call types TTY, fax, or modem that do not use pass-through mode: Enter the number of duplicated packets, from 0 to 3, that the system sends with each primary packet in the call. A value of 0 means that you do not want to send duplicated packets.
    - For clear-channel call type and call types for which you selected the pass-through mode: Enter either 0 or 1. If you select 0, the system does not use redundant payloads. If you select 1, the system uses redundant payloads.
14. In the **Media Connection IP Address Type Preferences** field, enter any of the following:
    - `ipv4/ipv6`
    - `ipv6/ipv4`
    - `ip4/none`
    - `ipv6/none`
15. Save the changes.
16. Type any of the following and press `Enter`:
    - `list ip-codec-set`
    - `list ip-media-parameters`

    The system lists all codec sets on the CODEC Set screen.
17. Review the codec sets.

IP network regions

Use network regions to group IP endpoints and VoIP and signaling resources that share the same characteristics. Signaling resources includes Avaya Aura® Media Server and PROCR. In

this context, IP endpoint refers to IP stations, IP trunks, and G430 and G450 branch gateways. These IP endpoints and resources have the following characteristics:

- Audio Parameters
  - Codec Set
  - UDP port Range
  - Direct IP-IP connections
  - Hairpinning
- H.323 security profile
  - TLS service
    - Signaling channel encryption
  - TTS service
    - Registration and reregistration process

  Important:

  Communication Manager uses TLS to encrypt the signaling channel between Communication Manager and 96x1 H.323 phones. It also uses TTS for fast registration and reregistration process.
- Quality of Service Parameters:
  - Diffserv settings
    - Call Control per-hop behavior (PHB)
    - VoIP Media PHB
  - 802.1p/Q settings
    - Call Control 802.1p priority
    - VoIP Media 802.1p priority
    - VLAN ID
  - Better than Best Effort (BBE) PHB
  - RTCP settings
  - RSVP settings
  - Location
- WAN bandwidth limitations
  - Call Admission control - Bandwidth Limitation (CAC-BL)
  - Inter-Gateway Alternate Routing (IGAR)

For more information about ip-network-region, see *Administering Avaya Aura® Communication Manager*.

Note:

For more information about using network regions, with examples, see the application note Network Regions for Avaya MultiVantage™ Solutions at: http://www.support.avaya.com. For more information about configuring network regions in Communication Manager, see the application note *Avaya Aura® Communication Manager Network Region Configuration Guide*, at: http://www.support.avaya.com.

Defining an IP network region

About this task

Caution:

Never define a network region to span a WAN link.

Accept the default values for the following screen.

Procedure

1. Type `change ip-network-region`.

   The system displays the IP Network Region screen.

2. Complete the fields using the information in *IP Network Region field descriptions*.

3. Save the changes.

   Caution:

   If you change 802.1p/Q on the IP Network Region screen, the format of the Ethernet frames changes. 802.1p/Q settings in Communication Manager must match the settings in all interfacing elements in your data network.

IP Network Region field descriptions

Name	Description
NR Group	Use this field to assign a network region group to the network region. You can enter a value from: 1 to 2000 for large systems. 1 to 250 for small systems. **Note:** Do not leave the field blank. You can assign multiple network regions to the same network region group.
Region	Network Region number, 1–2000.

Table continues…

Name	Description
Location	Blank or 1–2000. If you leave the field blank, the system obtains the location from the PROCR that the endpoint is registered through. The system can also get the location from the gateway through which the endpoint is registered. The setting for the location field applies to IP telephones and softphones.
Name	The name of the region. Enter a character string up to 20 characters.
Authoritative Domain	The network domain of the server.
Stub Network Region	The network region that is a core network region or a stub network region. For network regions 251 to 2000, this field is a read-only field with a default value n. If you are creating a stub network region, you must enter more information on page 4, in the **dst rgn** field. Enter the number of the destination core network region that directly connects with this stub network region. **Note:** To convert a core network region to a stub network region, ensure that the core network region is connected with only one core network region. A stub network must have only one direct connection with a core network.
MEDIA PARAMETERS	
Codec Set	Specifies the codec set assigned to a region. Enter a value between 1-7. The default value is 1. **Note:** Codec sets are administered on the CODEC Set screen. See“ IP CODEC sets”.

Table continues…

Name	Description
UDP Port-Min	Specifies the lowest port number to be used for audio packets. Enter a value between 2-65406. The default is 2048. **Note:** This number must be twice the number of calls that must be supported plus one, must start with an even number, and must be consecutive. The minimum range is 128 ports. **Caution:** Do not use the range of well-known or IETF-assigned ports. Do not use ports below 1024.
UDP Port-Max	Specifies the highest port number to be used for audio packets. Enter a value between 130-65535. The default value is 65535. **Caution:** Do not use the range of well-known or IETF-assigned ports. Do not use ports below 1024.
DIFFSERVE/TOS PARAMETERS	
Call Control PHB Value	The decimal equivalent of the Call Control PHB value. Enter a value between 0-63. • Use PHB 46 for expedited forwarding of packets. • Use PHB 46 for audio for legacy systems that only support IPv4 Type-of-Service, which correlates to the older ToS critical setting. • Use PHB 46 if you negotiated a Call Control PHB value in your SLA with your Service Provider.
Audio PHB Value	The decimal equivalent of the VoIP Media PHB value. Enter a value between 0-63: • Use PHB 46 for expedited forwarding of packets. • Use PHB 46 for audio for legacy systems that only support IPv4 Type-of-Service, which correlates to the older ToS critical setting.
802.1p/Q PARAMETERS	
Call Control 802.1p Priority	Specifies the 802.1p priority value, and displays only if the **802.1p/Q Enabled** field is y. The valid range is 0–7. Avaya recommends 6 (high). See Caution below this table.

Table continues…

Name	Description
Audio 802.1p Priority	Specifies the 802.1p priority value, and displays only if the **802.1p/Q Enabled** field is y. The valid range is 0–7. Avaya recommends 6 (high). See Caution below this table.
Video 802.1p Priority	Specifies the Video 802.1p priority value, and displays only if the **802.1p/Q Enabled** field is y. The valid range is 0–7.
H.323 IP ENDPOINTS	
H.323 Link Bounce Recovery	Specifies whether to enable H.323 Link Bounce Recovery feature for this network region. Select y or n.
Idle Traffic Interval (sec)	Enter the maximum traffic idle time in seconds in the range 5-7200. Default is 20.
Keep-Alive Interval (sec)	Specify the interval between KA retransmissions in seconds. Enter a value in the range 1–120. The default value is 5.
Keep-Alive Count	Specify the number of retries if no ACK is received. Enter a value in the range 1–20. The default value is 5.
Intra-region IP-IP Direct Audio	Enter `y`: To save on bandwidth resources and improve sound quality of voice over IP transmissions. Enter `native (NAT)`: If the IP address from which audio is to be received for IP-to-IP connections within the region is that of the IP telephone/IP Softphone. Ensure that the IP address has not been translated by NAT. IP telephones must be configured behind a NAT device before this entry is enabled. Enter `translated (NAT)`: If the IP address from which audio is to be received for IP-to-IP connections within the region is the address with which a NAT device replaces the native address. IP telephones must be configured behind a NAT device before this entry is enabled.

Table continues…

Name	Description
Inter-region IP-IP Direct Audio	Enter `y` to save on bandwidth resources and improve sound quality of voice over IP transmissions. Enter `translated (NAT)` if the IP address from which audio is to be received for direct IP-to-IP connections between regions is to be the one with which a NAT device replaces the native address. IP telephones must be configured behind a NAT device before this entry is enabled. Enter `native (NAT)` if the IP address from which audio is to be received for direct IP-to-IP connections between regions is that of the telephone itself without being translated by NAT. IP telephones must be configured behind a NAT device before this entry is enabled.
IP Audio Hairpinning?	Enter `y` for IP endpoints to be connected through the server's IP circuit pack in IP format, without first going through the Avaya TDM bus.
AUDIO RESOURCE RESERVATION PARAMETERS	
RSVP Enabled?	Specifies whether or not you have to enable RSVP. Enter y or n.
RSVP Refresh Rate (sec)	Enter the RSVP refresh rate in seconds 1-99. This field only displays if the **RSVP Enabled** field is set to y.
Retry upon RSVP Failure Enabled	Specifies whether to enable retries when RSVP fails. Enter y or n. This field only displays if the **RSVP Enabled** field is set to y.
RSVP Profile	This field only displays if the **RSVP Enabled** field is set to y. You set this field to what you have configured on your network: • guaranteed-service makes a limit on the end-to-end queuing delay from the sender to the receiver. This setting is the most appropriate setting for VoIP applications. • controlled-load, a subset of guaranteed-service, provides for a traffic specifier but not the end-to-end queuing delay.

Table continues…

Name	Description
RSVP unreserved (BBE) PHB Value	Provides scalable service discrimination on the Internet without per-flow state and signaling at every hop. Enter the decimal equivalent of the DiffServ Audio PHB value, 0-63. This field only displays if the **RSVP Enabled** field is set to y. **Note:** The per-flow state and signaling is RSVP. When RSVP is not successful, the BBE value is used to discriminate between Best Effort and voice traffic that has attempted to get an RSVP reservation, but failed.
RTCP Reporting to Monitor Server Enabled	If enabled, sends RTCP Reports to a special server, such as for the VMON tool. **Note:** Regardless of how this field is administered, RTCP packets are always sent peer-to-peer
RTCP MONITOR SERVER PARAMETERS	
IPV4 Server Port	Available only if RTCP Reporting is enabled and if Default Server Parameters are disabled. • Valid entry: 1 to 65535 • Usage: The port for the RTCP Monitor server. Default is 5005.
IPV6 Server Port	Available only if RTCP Reporting is enabled and if Default Server Parameters are disabled. • Valid entry: 1 to 65535 • Usage: The port for the RTCP Monitor server. Default is 5005.
RTCP Report Period (secs)	Available only if RTCP Reporting is enabled and if Default Server Parameters are disabled. • Valid entry: 5 to 30 • Usage: The report period for the RTCP Monitor server in seconds.
Server IPV4 Address	The IPv4 address for the RTCP Monitor server. Available only if RTCP Reporting is enabled and if Default Server Parameters are disabled.
Server IPV6 Address	The IPv6 address for the RTCP Monitor server. Available only if RTCP Reporting is enabled and if Default Server Parameters are disabled.

Table continues…

Name	Description
Use Default Server Parameters	If enabled, uses the system-wide default RTCP Monitor server parameters. Available only if RTCP Reporting is enabled.
ALTERNATIVE NETWORK ADDRESS TYPES	
ANAT Enabled	Use this field to control the call processing behavior to send Alternative Network Address Types (ANAT) offer system wide. The valid entries are: • y: Communication Manager sends ANAT offer irrespective of the ip-network-region system wide setting. • n: Communication Manager does not send ANAT offer irrespective of the ip-network-region system wide setting.
INTER-GATEWAY ALTERNATE ROUTING/DIAL PLAN TRANSPARENCY	If **Inter-Gateway Alternate Routing** (IGAR) is enabled for any row on subsequent pages, the following fields for each network region must be administered to route the bearer portion of an IGAR call.
Conversion to Full Public Number - Delete	• Valid entry: 0 to 7 • Usage: The digits to delete.
Conversion to Full Public Number - Insert	• Valid entry: 0 to 13 or blank • Usage: The number of digits to insert. International numbers should begin with plus (+). The Inter-Gateway Alternate Routing (IGAR) and Dial Plan Transparency (DPT) features convert the plus (+) digit to appropriate international access code when starting the trunk call. **Note:** The optional plus (+) at the beginning of the inserted digits is an international convention indicating that the local international access code must be dialed before the number.
Dial Plan Transparency in Survivable Mode	The valid entries are: • y: Enables the Dial Plan Transparency feature when a gateway registers with a Survivable Remote Server (Local survivable processor), or when a port network registers with a Survivable Core Server (Enterprise Survivable Server). • n: Default is n.

Table continues…

Name	Description
Incoming LDN Extension	An extension used to assign an unused Listed Directory Number for incoming IGAR calls.
Maximum Number of Trunks to Use for IGAR	It is necessary to impose a limit on the trunk usage in a particular port network in a network region when Inter-Gateway Alternate Routing (IGAR) is active. The limit is required because if there is a major IP WAN network failure, it is possible to use all trunks in the network region(s) for IGAR calls. • Valid entry: 1 to 999, or blank • Usage: The maximum number of trunks to be used for Inter-gateway alternate routing (IGAR).
BACKUP SERVERS IN PRIORITY ORDER	Lists the backup server names in priority order. Backup server names should include Survivable Remote Server names and Survivable Core Server names. If you are using the Processor Ethernet, the backup servers list must include the survivable core PE address else the phones will not register to the survivable core during a failure. Any valid node name is a valid entry. Valid node names can include names of Customer LANs, ICCs, Survivable Core Servers, and Survivable Remote Servers.
H.323 SECURITY PROFILES	Permitted security profiles for endpoint registration in the network region. You must enter at least one security profile. Otherwise, no endpoint will be permitted to register from the region. The valid entries are: • challenge: Includes the various methods of PIN-based challenge and response schemes in current use. This is a relatively weak security profile. • pin-eke: The H.235 Annex H SP1 • strong: Permits the use of any strong security profile. The `H323TLS` profile is the strongest security profile in Communication Manager. • any-auth: Includes any of the security profiles. • H323TLS: Communication Manager apples this security profile when the network region of an H. 323 phone is administered with H323TLS or Strong security profiles. Also, Communication Manager and the endpoint negotiate by using the H323 TLS profile. H323TLS profile sends H.323 signaling messages through a TLS-encrypted channel.

Table continues…

Name	Description
Allow SIP URI Conversion	Administers whether or not a SIP URI should be permitted to change. Degrading the URI from sips//: to sip//: might result in a less secure call. This is required when SIP SRTP endpoints are allowed to make and receive calls from endpoints that do not support SRTP. The valid entries are: • y: Allows conversion of SIP URIs. Default is y. • n: No URI conversion. Calls from SIP endpoints that support SRTP made to other SIP endpoints that do not support SRTP will fail. However, if you enter y for the **Enforce SIPS URI for SRTP** field on the signaling group screen, URI conversion takes place independent of the value set for the **Allow SIP URI conversion** field on the IP Network Region screen.
TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS	
Near End Establishes TCP Signaling Socket	Indicates whether Communication Manager (the near end) can establish the TCP socket for H.323 IP endpoints in this network region. The valid entries are: • y: Communication Manager determines when to establish the TCP socket with the IP endpoints, assuming the endpoints support this capability. This is the default. • n: The IP endpoints always attempt to set up the TCP socket immediately after registration. This field should be disabled only in network regions where a nonstandard H.323 proxy device or a non-supported network address translation (NAT) device would prevent the server from establishing TCP sockets with H.323 IP endpoints.
Near End TCP Port Min	• Valid entry: 1024 to 65531 • Usage: The minimum port value used by the processor Ethernet when establishing the TCP signaling socket to the H.323 IP endpoint. The range of port number must be at least 5 (Max-Min+1). Default is 61440.

Table continues…

Name	Description
Near End TCP Port Max	• Valid entry: 1028 to 65535 • Usage: The maximum port value to be used by the processor Ethernet when establishing the TCP signaling socket to the H.323 IP endpoint. The range of port number must be at least 5 (Max-Min+1). Default is 61444.
AGL	The maximum number of destination region IP interfaces included in alternate gatekeeper lists (AGL). The valid entries are: • 0 to 16: Communication Manager uses the numeric value of gatekeeper addresses. • 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. • blank: The administration field is ignored.
codec-set	• Valid entry: 1 to 7, pstn, or blank • Usage: The codec set used between the two regions. This field cannot be blank if this route through two regions is being used by some non-adjacent pair of regions. If the two regions are disconnected at all, this field should be blank.
direct-WAN	Indicates whether the two regions (source and destination) are directly connected by a WAN link. The default value is enabled if a **codec-set** is administered.
dst rgn	• Valid entry: 1 to 250 • Usage: The destination region for this inter-network connection.
Dyn CAC	Available only if the **WAN-BW-limits (Units)** is Dynamic. The gateway must be configured to be a CAC (Call Admission Control) gateway. • Valid entry: 1 to 250, or blank • Usage: The gateway that reports the bandwidth-limit for this link. Default is blank. **Note:** If you set the **BW Management Option** field to shared-SM, you cannot view this field.

Table continues…

Name	Description
IGAR	Allows pair-wise configuration of Inter-Gateway Alternate Routing (IGAR) between network regions. The valid entries are: • y: Enables IGAR capability between this network region pair. Default for a pstn codec set. • n: Disable IGAR capability between this network region pair. Default, except for a pstn codec set. • f: Forced. Moves all traffic onto the PSTN. This option can be used during initial installation to verify the alternative PSTN facility selected for a network region pair. This option can also be used to temporarily move traffic off of the IP WAN if an edge router is having problems or an edge router needs to be replaced between a network region pair.
Intervening-regions	Allows entry of intervening region numbers between the two indirectly-connected regions. • Valid entry: 1 to 250 • Usage: Up to four intervening region numbers between the two indirectly-connected regions. **Note:** Indirect region paths cannot be entered until all direct region paths have been entered. In addition, the order of the path through the regions must be specified starting from the source region to the destination region.

Table continues…

Name	Description
Mtce	The valid entries are: • t: This is a test-only option. Inter-region connectivity testing is performed for the network region pair by using a simple PING sent between entities in each network region. If a test fails, only an error is added to the system error log. IP media connections between the region pair are never blocked. The testing is done at the rate of not more than once per 5 minutes. • m: This is a measurement based option. Inter-region connectivity testing is performed by a continuous set of PINGs sent between entities in each network region. The Ping Test Interval (sec) and Number of Pings Per Measurement Interval fields control the rate of testing. The Roundtrip Propagation Delay (ms) and Packet Loss (%) thresholds control success or failure. If the, test measurements exceed the administered thresholds; future IP media connections between the network region pair will be blocked. • d: No testing is performed for the network region pair.
src rgn	• Valid entry: 1 to 250 • Usage: The source region for this inter-network connection.
Sync	The system displays Sync when the **Synchronization over IP** field is enabled. The valid entries are: • y: Timing IGC streams are allowed between the region pair that is being administered. The default value is y. • n: Do not allow timing IGC streams between the region pair that is being administered.
Video (Norm)	• valid entry: 0 to 9999 for Kbits, 0 to 65 for Mbits, or blank for NoLimit • Usage: The amount of bandwidth to allocate for the normal video pool to each IP network region. **Note:** If you set the **BW Management Option** field to shared-SM, you cannot view this field.

Table continues…

Name	Description
Video (Prio)	• Valid entry: 0 to 9999 for Kbits, 0 to 65 for Mbits, or blank for NoLimit • Usage: The amount of bandwidth to allocate for the priority video pool to each IP network region. **Note:** If you set the **BW Management Option** field to shared-SM, you cannot view this field.
Video (Shr)	Specifies whether the normal video pool can be shared for each link between IP network regions. **Note:** If you set the **BW Management Option** field to shared-SM, you cannot view this field.
WAN-BW limits (Total)	The valid entries are: • 1 to 9999: The bandwidth limit for direct WAN links. Values for this field can be entered in the number of connections, bandwidth in Kbits or calls, or left blank for NoLimit. • 1 to 65: Values for this field can be entered in the number of connections, bandwidth in Mbits, or left blank for NoLimit. **Note:** If you set the **BW Management Option** field to shared-SM, you cannot view this field.
WAN-BW-limits (Units)	• Valid entry: Calls, Dynamic, Kbits/sec, Mbits/sec, or blank for NoLimit • Usage: The unit of measure corresponding to the value entered for bandwidth limitation. Bandwidth should be limited by the number of connections, bandwidth in Kbits/sec, or bandwidth in Mbits/sec, or left blank. Default is blank. **Note:** If you set the **BW Management Option** field to shared-SM, you cannot view this field.

Call Admission Control

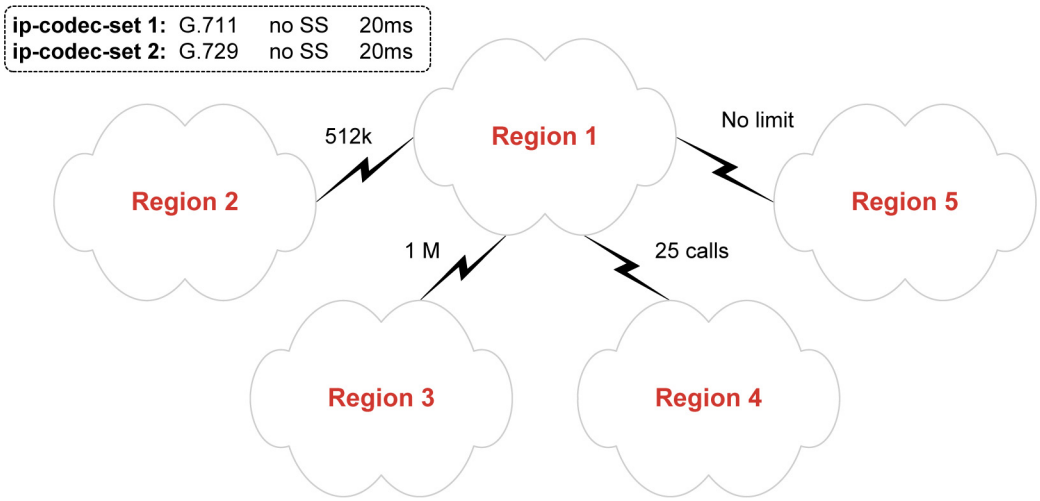
Call Admission Control (CAC) is a feature to set a limit on the bandwidth consumption or number of calls between network regions.

Note:

If SRTP media encryption is used for SIP and H.323 calls, CAC must be adjusted for the additional overhead imposed by the authentication process. SRTP authentication can add 4 (HMAC32) or 10 (HMAC80) bytes to each packet.

The primary use of this feature is to prevent WAN links from being overloaded with too many calls. To use CAC, set either a bandwidth limit or a number-of-calls limit between network regions, as follows:

- Bandwidth consumption is calculated using the methodology explained in *Avaya Aura® Core Solution Description*.
- The L2 overhead is 7 bytes, which is the most common L2 overhead size for WAN protocols.
- The calculated bandwidth consumption is rounded up to the nearest whole number.
- The calculated bandwidth consumption takes into account the actual IP codec being used for each individual call. All calls do not use the same codec.
- If the administrator chooses not to have the server calculate the bandwidth consumption, the user can enter a manual limit for the number of calls. However, this manually entered limit is adhered to regardless of the codec being used. Therefore, the administrator must be certain that all calls use the same CODEC, or that the manual limit calculates the highest possible bandwidth consumption for the specified inter-region codecset.
- If a call between two network regions traverses an intervening network region, the call server keeps track of the bandwidth consumed across both inter-region connections.



- With the Call Admission Control (CAC) sharing between Communication Manager and Session Manager feature, Session Manager acts as the central authority for bandwidth management. Communication Manager obtains bandwidth for voice and multimedia IP connections from Session Manager.

The figure above shows a simple hub-spoke network region topology. The WAN link between network regions 1 and 2 has 512 kbps reserved for VoIP. The WAN link between network regions 1 and 3 has 1 Mbps reserved for VoIP. The link between network regions 1 and 4 is one where the 7-byte L2 overhead assumption cannot hold, such as an MPLS or VPN link. In this case, the

administration is such that all inter-region calls terminating in region 4 use the G.729 codec (with no SS at 20 ms).

Therefore, you can set a limit on the number of inter-region calls to region 4. You must know exactly how much bandwidth that CODEC consumes with the MPLS or VPN overhead added. Finally, the link between network regions 1 and 5 requires no limit, either because there are very few endpoints in region 5 or because there is practically unlimited bandwidth to region 5.

The corresponding IP Network Region screens for each network region are shown below.

```
change ip-network-region 1                                    Page   3 of  19

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                    G   A     e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A   G     a
 rgn  set   WAN  Units     Total Norm  Prio Shr Regions          CAC  R   L     s
 1    1                                                             all
 2    3     y    Kbits    2000  1000   0   y                        n   ___
 3    1     y    NoLimit                                          n   ___
 4    1     y    NoLimit                                          n   ___
 5    4     y    Kbits    4096  1088   0   y                        n   ___
 6    1     y    NoLimit                                          n   ___
 7    _____                                                         ___
 8    _____                                                         ___
 9    _____                                                         ___
 10   _____                                                         ___
 11   _____                                                         ___
 12   _____                                                         ___
 13   _____                                                         ___
 14   _____                                                         ___
 15   _____                                                         ___
```

```
change ip-network-region 2                                    Page   3 of  19

 Source Region: 2     Inter Network Region Connection Management      I       M
                                                                     G   A     e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn   A   G     a
 rgn  set   WAN  Units     Total Norm  Prio Shr Regions          CAC   R   L     s
 1    3     y    Kbits    2000  1000   0   y                        n   ___
 2    1                                                             all
 3    2     y    NoLimit                                          n   ___
 4    _____                                                         ___
 5    _____                                                         ___
 6    _____                                                         ___
 7    _____                                                         ___
 8    _____                                                         ___
 9    _____                                                         ___
 10   _____                                                         ___
 11   _____                                                         ___
 12   _____                                                         ___
 13   _____                                                         ___
 14   _____                                                         ___
 15   _____                                                         ___
```

```
change ip-network-region 3                                    Page   3 of  19

 Source Region: 3     Inter Network Region Connection Management      I       M
                                                                     G   A     e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn   A   G     a
 rgn  set   WAN  Units     Total Norm  Prio Shr Regions          CAC   R   L     s
 1    1     y    NoLimit                                          n   ___
 2    2     y    NoLimit                                          n   ___
 3    1                                                             all
 4    _____                                                         ___
 5    _____                                                         ___
 6    _____                                                         ___
 7    _____                                                         ___
 8    _____                                                         ___
 9    _____                                                         ___
 10   _____                                                         ___
 11   _____                                                         ___
 12   _____                                                         ___
 13   _____                                                         ___
 14   _____                                                         ___
 15   _____                                                         ___
```

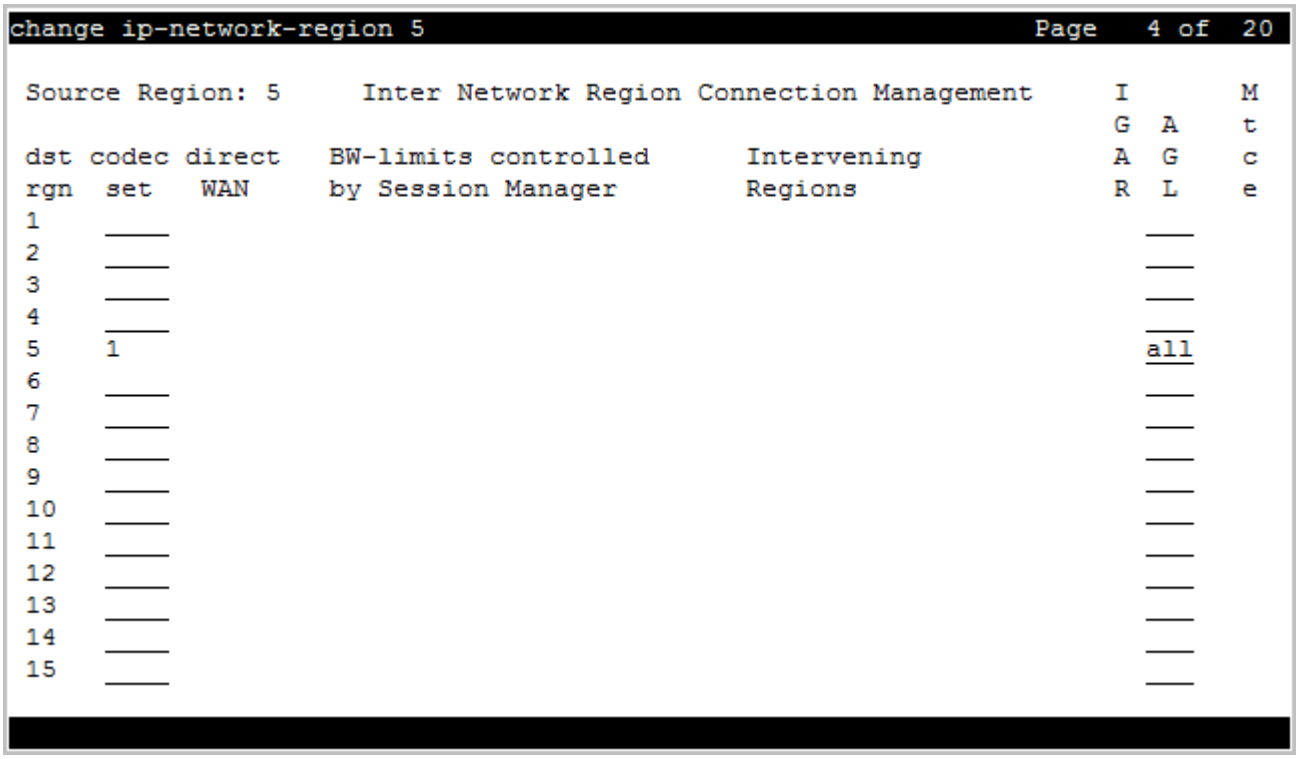
```
change ip-network-region 4                                    Page   3 of  19

 Source Region: 4     Inter Network Region Connection Management      I       M
                                                                     G   A     e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn   A   G     a
 rgn  set   WAN  Units     Total Norm  Prio Shr Regions          CAC   R   L     s
 1    1     y    NoLimit                                            n
 2
 3
 4    1                                                               all
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
```

```
change ip-network-region 5                                    Page   3 of  19

 Source Region: 5     Inter Network Region Connection Management      I       M
                                                                     G   A     e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn   A   G     a
 rgn  set   WAN  Units     Total Norm  Prio Shr Regions          CAC   R   L     s
 1    4     y    Kbits    4096  1088    0   y                        n
 2
 3
 4
 5    5                                                               all
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
```

Following is the screenshot of the screen when you set the **BW Management Option** field to shared-SM.



```
change ip-network-region 5                                    Page   4 of  20

Source Region: 5     Inter Network Region Connection Management     I       M
                                                                   G  A    t
dst codec direct   BW-limits controlled      Intervening           A  G    c
rgn  set   WAN     by Session Manager        Regions               R  L    e
1    _____                                                           ___
2    _____                                                           ___
3    _____                                                           ___
4    _____                                                           ___
5    1                                                               all
6    _____                                                           ___
7    _____                                                           ___
8    _____                                                           ___
9    _____                                                           ___
10   _____                                                           ___
11   _____                                                           ___
12   _____                                                           ___
13   _____                                                           ___
14   _____                                                           ___
15   _____                                                           ___
```

Administering DPT

Procedure

1. On the SAT screen, type `change system-parameters features` and press `Enter`.

   The system displays the Feature-Related System Parameters screen.
2. In the **Enable Dial Plan Transparency in Survivable Mode** field, type `y`.
3. In the **COR to Use for DPT** field, type one of the following values:
   - `station`: With this setting, the Facility Restriction Level (FRL) of the calling station determines whether that station is permitted to make a trunk call. The FRL also determines the trunks that the calling station is eligible to access.
   - `unrestricted`: With this setting, the first available trunk preference determined by ARS routing is used.
4. Save and exit the screen.
5. On the SAT screen, type `change ip-network-region` *number*, where *number* is the ip network region number.

   The system displays the IP Network Region screen.
6. In the **Dial Plan Transparency in Survivable Mode** field, type `y`.

7. Allocate an incoming DID or LDN extension for incoming DPT calls.

   This extension can be shared by IGAR and DPT.

8. Ensure that enough trunks are available for IGAR.

   You do not need to set the maximum number of trunks for DPT.

9. Use existing routing techniques to ensure that an outgoing DPT call from a specified network region has access to an outgoing trunk.

   The outgoing trunk need not be in the same network region as the calling endpoint if the endpoint and trunk network regions are interconnected.

Manually interconnecting the network regions

You can enable IGAR using the **Enable Inter-Gateway Alternate Routing** field on the Feature-Related System Parameters screen.

If PROCR, G4xx Media Gateway, and Avaya Aura® Media Server resources are shared among administered network regions, on the Inter-Network Region Connection Management screen, define the following:

- Which regions communicate with which other regions.
- Which codec set is used for inter-region communication.

Note:

Specify the codec set on the Inter-Network Region Connection Management screen before connecting IP endpoints in different network regions or communicating among network regions.

For the Call Admission Control - Bandwidth Limitation feature, you can also specify:

- Whether regions are directly connected or indirectly connected through intermediate regions.
- Bandwidth limits for IP bearer traffic between two regions by using a maximum bit rate or number of calls.

  When a bandwidth limit is reached, more IP calls between those regions are diverted to other channels or blocked.

  When the codec set administered across a WAN link contains a single codec, the bandwidth limit is specified as the number of calls. When the codec set administered across a WAN link contains multiple codecs, the bandwidth limit is usually specified as a bit-rate. For regions connected across a LAN, the normal bandwidth limit setting is no limit.

For more information about using network regions, see *Network Regions for Avaya MultiVantage™ Solutions* at: http://www.support.avaya.com. For more information about configuring network regions in Communication Manager, see *Avaya Aura® Communication Manager Network Region Configuration Guide*, at: http://www.support.avaya.com. For information about using the Network Region Wizard, see *Network Region Job Aid* at: http://support.avaya.com.

Internetwork region connections

The **Alternate Routing Extension** field is available on the IP Network Region screen. Each network region uses this field, which is up to 7 digits long, to route the bearer portion of the IGAR call.

If IGAR is enabled for any row on pages 3 through 19, then the user must enter an IGAR extension before submitting the screen. Also, the user is blocked from blanking out a previously administered IGAR extension. If IGAR is disabled by the System Parameter, the customer is warned when any of these fields are updated.

Warning:

The IGAR System Parameter is disabled.

Pair-wise administration of IGAR between network regions

An IGAR column is added to the IP Network Region screen for pair-wise configuration of IGAR between network regions. If the field is set to `y`, the IGAR capability is enabled between the specific network region pair. If the field is set to `n`, the IGAR capability is disabled between the network region pair.

The following screen validations must be performed:

- When IGAR Extension is not administered on page 2 of the IP Network Region screen, the user is blocked from submitting the screen. The user is blocked if any network region pair has IGAR enabled.
- When IGAR is disabled using the System Parameter, the customer is warned if IGAR is enabled for any network region pair.

  The system displays the following warning:

  ```
  WARNING: The IGAR System Parameter is disabled.
  ```

Normally, the administration between Network Region pairs can have a codec set identified for compressing voice across the IP WAN. However, if the IP WAN bandwidth is exceeded, and the **IGAR** field is set to `y`, the voice bearer is routed across an alternate trunk facility. However, under some conditions, you can force all calls to the PSTN.

The forced option can be used during initial installation to verify the alternative PSTN facility selected for a Network Region pair. This option can also be used to move traffic off the IP WAN temporarily. For example, the option is useful if an edge router is having problems, or an edge router must be replaced between a network region pair.

When the codec set type is `pstn`, the system uses `y` as the default value for the **IGAR** field. This default value must be used because Alternate Trunk Facility is the only means of routing the voice bearer part of the call. The other values permitted for this field are f(orced) and n(o).

When the codec set is set to `pstn`, the following fields are hidden:

- Direct-WAN
- WAN-BW Limits

- Intervening Regions

When the codec set is not `pstn` and not blank, the system uses `n` as the default value for the **IGAR** field.

```
change ip-network-region 3                                    Page 4 of 20

                    Inter Network Region Connection Management          I          M
                                                                        G    A     t
dst   codec direct   WAN-BW-limits   Video       Intervening    Dyn     A    G     c
rgn    set   WAN  Units     Total Norm  Prio Shr Regions        CAC     R    L     e
 1      1___  y    256:Kbits__  __________      ___  ___  ___  ___     f
 2      1___  n    ___________  __________      1__  ___  ___  ___     y
 3      1___  _    ___________  __________      ___  ___  ___  ___     n
 4      1___  n    ___________  __________      1__  ___  ___  ___     n
 5      1___  n    ___________  __________      6__  ___  ___  ___     y
 6      1___  _    ___:NoLimit  __________      ___  ___  ___  ___     y
 7      1___  y    _10:Calls__  __________      ___  ___  ___  ___     n
 8      pstn  _    ___________  __________      ___  ___  ___  ___     y
 9      pstn  _    ___________  __________      ___  ___  ___  ___     y
 10
 11
```

Figure 9: Internetwork region connection management

Specify codec sets for your shared network regions by putting a codec set number in the **codec-set** column. Specify the inter-region connections and bandwidth limits in the remaining columns.

In this example, network region 3 is connected to regions 6 and 7. Network region 3 is indirectly connected to regions 2 and 4 through region 1, and 5 through region 6.

G4xx Media gateways to network region mapping for media modules

The critical non-IP boards of interest are the trunk media modules over which IGAR calls are routed. In some instances, the system cannot establish an IP connection between two media gateways. Then, the system tries to establish an IGAR trunk connection between the two MGs. The system tries to use trunks in the specific MG requested. However, because Communication Manager does not require every MG to have PSTN trunks, you must get trunks from another MG. The system can only get trunks from a MG in the same network region as the one in which the original request was made.

Status of interregion usage

You can check the status of bandwidth usage between network regions with the following commands:

- **`status ip-network-region`** *n*, where *n* is the network region number
- **`status ip-network-region`** *n/m*

With the **`status ip-network-region`** *n* command, the system displays the Inter Network Region Bandwidth Status screen.

Note:

If you set the **BW Management Option** field to shared-SM, you cannot run this command. The system displays the message: `Consult SMGR for bandwidth status.`

When you run the **`status ip-network-region`** *n* command, the connection status, bandwidth limits, and bandwidth usage is displayed for all regions directly connected to *n*. For regions indirectly connected to *n*, only the connection status is displayed. If regions *n* and *m* are indirectly connected, using *n/m*, the command displays the connection status, bandwidth limits, and bandwidth usage for each intermediate connection.

The **IGAR Now/Today** column on the Inter Network Region Bandwidth Status screen displays the number of times IGAR is used for a network region pair.

```
status ip-network-region 2
                  Inter Network Region Bandwidth Status
                                                 Number of   # Times
Src Dst Conn     Conn  BW-Limit  BW-Used(Kbits) Connections  BW-Limit  IGAR
Rgn Rgn Type     Stat               Tx    Rx     Tx    Rx   Hit Today Now/Today
2   1   direct   pass  128 Kbits    xxx   xxx   xxx   xxx     xxx     xxx/ xxx
              Video:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
           Priority:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
2   3   indirect pass  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
              Video:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
           Priority:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
2   4   indirect pass  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
              Video:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
           Priority:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
2   11  indirect pass  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
              Video:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
           Priority:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
```

Figure 10: IP network region status screen

Following is the screenshot of the screen when you set the **BW Management Option** field to shared-SM.

```
status ip-network-region 5

Enter region number (1-2000) or [src/dest region numbers]

Or press CANCEL to cancel the command




Consult SMGR for bandwidth status
```

The numbers in the column titled **IGAR Now/Today** indicate the following :

- The first number displays the number of active IGAR connections for the pair of network regions at the time the command is invoked. This number is up to 3 digits long or 999.
- The second number displays the number of times IGAR is used for the pair of network region since the previous midnight. This number is up to 3 digits long or 999.

Administering the network region on the Signaling Group screen

Procedure

1. On the SAT screen, type `change signaling-group` *group number* and press `Enter`.

   The system displays the Signaling Group screen.

2. In the **Far-end Network Region** field, type the number of the network region that corresponds to this signaling group.

   The network region number has a value in the range 1-250.

3. Press `Enter`.

   The system saves the changes.

Reviewing the network region administration

Procedure

1. Type `busy signaling-group` *number*.

   The signaling group is now in busy-out state.

2. Type `change signaling-group` *number*.

   The system displays the Signaling Group screen.

3. In the **Trunk Group for Channel Selection** field, type the trunk group number.

   When more than one trunk group is assigned to this signaling group, enter the group that accepts incoming calls.

4. Save the changes.

5. Type `release signaling-group` *number*.

   The signaling group is released.

Setting network performance thresholds

About this task

You require a craft login or a higher login to perform this administration.

Communication Manager provides control over four IP media packet performance thresholds to streamline VoIP traffic. You can use the default values for these parameters, or you can change the values to fit the needs of your network. These threshold values apply only to IP trunks and do not affect other IP endpoints.

Procedure

1. On the SAT screen, type `change signaling-group` *n*.

2. On the Signaling Group screen, in the Group Type field, type `h.323` or `sip`.

3. In the **Bypass If IP Threshold Exceeded** field, type `y`.

   If bypass is activated for a signaling group, the system compares the ongoing measurements of network activity with the values in the IP-options system-parameters screen. If the current measurements exceed the values in the IP-options system-parameters screen, the bypass function terminates use of the network path for the signaling group. The following actions are taken when thresholds are exceeded:

   - Existing calls on the IP trunk associated with the signaling group are not maintained.
   - Incoming calls do not arrive at the IP trunks on the bypassed signaling group and are diverted to alternate routes.
   - Outgoing calls are blocked on this signaling group.

     If so administered, blocked calls are diverted to alternate routes, either IP or circuits, as determined by the administered routing patterns.

     Note:

     Use the default values.

Administering network performance parameters

Procedure

1. On the SAT screen, type `change system-parameters ip-options`.

   The system displays the IP Options System Parameters screen.

2. In the **Roundtrip Propagation Delay (ms)**, **Packet Loss (%)**, **Ping Test Interval (sec)**, and **Number of Pings per Measurement Interval** fields, type appropriate values.

   The default values for these fields are:

   - Roundtrip Propagation Delay (ms): High: 800, Low: 400
   - Packet Loss (%): High: 40, Low: 15
   - Ping Test Interval (sec): 20
   - Number of Pings per Measurement Interval: 10

     10

   You can change these values to suit the requirements of the network.

3. Save the changes.

Enabling or disabling spanning tree

Procedure

1. On the P330 stack processor, open a telnet session using the serial cable connected to the Console port of the G4XX.
2. At the P330-x(super)# prompt, type `set spantree help` and press `Enter`.

   The system displays the Set spantree commands screen.

   Figure 11: Set Spantree commands on page 108 shows the full set of Spanning Tree commands.

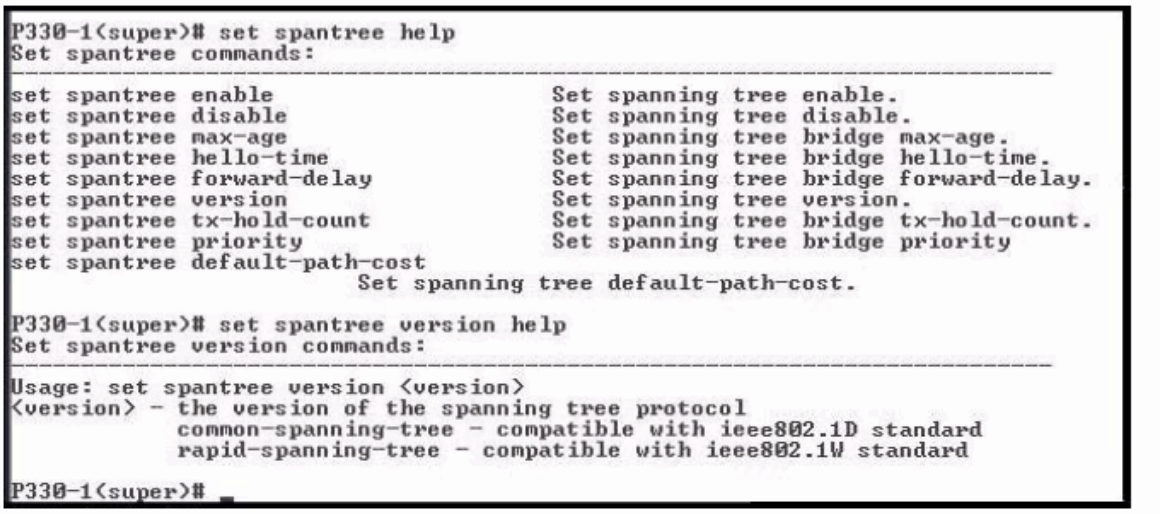


Figure 11: Set Spantree commands

3. To enable Spanning Tree, type `set spantree enable` and press `Enter`.
4. To set the version of Spanning Tree, type `set spantree version help` and press `Enter`.

   The system displays the selection of Spanning Tree protocol commands.
5. To set the rapid spanning tree version, type `set spantree version rapid-spanning-tree` and press `Enter`.

   The 802.1w standard defines the default path cost for a port different from STP (802.1d). To avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost with the **`set port spantree cost auto`** command.

   Note:

   Avaya P330s now support a Faststart or Portfast function because the 802.1w standard defines the support for these functions. An edge port goes to a device that cannot form a network loop. To set an edge port, type `set port edge admin statemodule/port edgeport`.

   For more information about the Spanning Tree CLI commands, see the *Avaya P330 User's Guide* at http://support.avaya.com.

Jitter buffers

Jitter buffers must not be more than twice the size of the largest statistical variance between packets because network packet delay is usually a factor. The best solution is to have dynamic jitter buffers that change size in response to network conditions. Avaya equipment uses dynamic jitter buffers.

Jitter can occur because of the following factors:

- Network congestion
- Insufficient bandwidth
- Route changes that can interact with network congestion or lack of bandwidth

UDP ports

With Communication Manager, you can configure User Datagram Protocol (UDP) port ranges that are used by VoIP packets. Network data equipment uses these port ranges to assign priority throughout the network. When the endpoint installer or user does not provide values for the UDP port ranges, Communication Manager can download default values to the endpoint.

Media encryption

Communication Manager supports encryption for IP bearer channel voice data transported in Real Time Protocol (RTP) between any combination of gateways and IP endpoints. Encryption provides privacy for media streams carried over the IP network

Digitally encrypting the audio or voice portion of a VoIP call can reduce the risk of electronic eavesdropping. IP packet monitors, sometimes called sniffers, are similar to wiretaps for circuit-switched (TDM) calls. However, an IP packet monitor can monitor and capture unencrypted IP packets and play back the conversation in real-time or store it for later playback.

With media encryption enabled, Communication Manager encrypts IP packets before the packets traverse the IP network. An encrypted conversation sounds like white noise or static when played through an IP monitor. End users do not know that a call is encrypted because:

- Visual or audible indicators are not present to indicate that the call is encrypted.
- Encrypted calls and nonencrypted calls do not differ in voice quality.

Limitations of media encryption

Security alert:

Ensure that you understand these important media encryption limitations:

- Any call that involves a circuit-switched (TDM) endpoint, such as a DCP or analog telephone, is vulnerable to conventional wire tapping techniques.
- Any call that involves an IP endpoint or gateway that does not support encryption can be a potential target for IP monitoring. Common examples are IP trunks to third-party vendor switches.
- Any party that is not encrypting an IP conference call exposes parties on the IP call between the unencrypted party and the supporting media processor to monitoring. This vulnerability can occur although the other IP links are encrypting.

Types of media encryption

Communication Manager supports the following Secure Real Time Protocol (SRTP) encryption profiles:

- srtp-aescm128
- srtp-aescm256
- None

License file

Media Encryption does not work unless the server has a valid license file with Media Encryption enabled. If Media Encryption is not enabled in the current license file, install a license file with Media Encryption enabled.

Determining whether media encryption is enabled in the current License File

Procedure

1. Type `display system-parameters customer-options` and press `Enter`.

   The system displays the Optional Features screen.

2. Go to the page with the **Media Encryption Over IP?** field and verify that the value is `y`.

   Note:

   In the U. S. and other countries, media encryption is enabled by default, unless prohibited by export regulations.

Administering media encryption for IP codec sets

Before you begin

The **Media Encryption** field is displayed on the IP Media Parameters screen only when:

- The Media Encryption over IP feature is enabled in the license file.
- The Media Encryption over IP feature is displayed as `y` on the Customer Options screen.

If the **Media Encryption Over IP?** field is set to `n`, the **Media Encryption** field on the IP Media Parameters screen is hidden and functions as if `none` is selected.

About this task

On the IP Media Parameters screen, you can administer the type of media encryption, if any, for each codec set.

Note:

H.323 endpoints do not require any encryption administration, and end users need not do anything to use media encryption

For information about SIP endpoints, see *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*

Procedure

1. On the SAT screen, type any of the following and press `Enter`:
   - `change ip-codec-set` *number*
   - `change ip-media-parameters` *number*

   The system displays the IP Media Parameters screen.
2. Enter up to three media encryption types.

   The **Media Encryption** field specifies one, two, three, four, or five options for the negotiation of encryption. In this exam, you can choose one mode each from SRTP, aes, and aea. You can specify no encryption by entering `none` in the **Media Encryption** field. The default value for this field is `none`. The order in which the options are listed signifies the preference of use, similar to the list of codecs in a codec set. Two endpoints must support at least one common encryption option for a call to be completed between them.

   Note:

   The option that you select in the **Media Encryption** field for each codec set applies to all codecs defined in the set.

Related links

IP Network Region field descriptions on page 83

Media encryption field description for IP codec set

Name	Description
aes	Advanced Encryption Standard (AES) is the standard cryptographic algorithm for U.S. government organizations to protect sensitive or classified information. Advanced Encryption Standard reduces circuit-switched-to-IP call capacity by 25%. AES is an Avaya proprietary technique and not recommended. Instead, use the following four SRTCP options: • 10-srtp-aescm256-hmac80 • 11-srtp-aescm256-hmac32 • 1-srtp-aescm128-hmac80 • 2-srtp-aescm128-hmac32

Table continues…

Name	Description
aea	Avaya Encryption Algorithm (AEA) is not as secure an algorithm as Advanced Encryption Standard, but call capacity reduction with Avaya Encryption Algorithm is negligible. Use this option as an alternative to Advanced Encryption Standard encryption when: • All endpoints within a network region using this codec set must be encrypted. • All endpoints communicating between two network regions and administered to use this codec set must be encrypted. AEA is an Avaya proprietary technique and not recommended. Instead, use the following four SRTCP options: • 10-srtp-aescm256-hmac80 • 11-srtp-aescm256-hmac32 • 1-srtp-aescm128-hmac80 • 2-srtp-aescm128-hmac32
SRTP-several encryption modes	AEA and AES encryption algorithms are not supported on SIP endpoints, use the following four SRTCP options: • 10-srtp-aescm256-hmac80 • 11-srtp-aescm256-hmac32 • 1-srtp-aescm128-hmac80 • 2-srtp-aescm128-hmac32
none	Media stream is unencrypted. This option prevents encryption when using this codec set and is the default setting when Media Encryption is not enabled.

Administering media encryption for H.323 signaling-groups

Before you begin

On the Customer Options screen, set the **Media Encryption Over IP?** field to `n`.

Procedure

1. Type `change signaling-group` *number*.

   The system displays the Signaling Group screen.

2. In the **Media Encryption?** field, type `y`.

   Media Encryption on trunk calls using this signaling group, is enabled.

Note:

If you leave this field with the default value n, the system overrides the encryption administration on the IP Media Parameters screen or any trunk call using this signaling group. The IP codec set used between two networks can be aes or aea. However, a call between two endpoints over an H.323 trunk using this IP codec set fails because there is no voice path.

3. In the **Passphrase** field, type an 8-character to 30-character string.

   This string must meet the following conditions:

   - Must contain at least one alphabetic and one numeric symbol.
   - Can include letters, numerals, and exclamation point (!), ampersand (&), asterisk (*), question mark (?), semicolon (;), single quotation mark ('), caret (^), opening parenthisis((), and closing parenthesis ()), dot (.), colon (:), and hyphen (-).
   - Is case-sensitive.

   You must administer the same passphrase on both signaling group forms at each end of the IP trunk connection. For example, if you have two systems A and B with trunk A-B between them, administer both Signaling Group forms with the same passphrase for the A-to-B trunk connection.

   If you administered a passphrase, a single asterisk (*) is displayed in this field. If you did not administer a passphrase, the field is blank.

   The **Passphrase** field does not appear if either the:

   - **Media Encryption Over IP?** field on the Customer Options screen is `n`.

     or

   - **Media Encryption?** field on the Signaling Group screen is `n`.

Viewing encryption status for stations and trunks

About this task

You can use the **`status station`** and **`status trunk`** commands to view the current status of encryption usage by stations and trunks.

Procedure

1. On the SAT screen, type `status station` *extension*, and go to the Connected Ports page.

   On the Connected Ports screen, you can see that a port is currently connected and using a G711 codec with SRTP media encryption.

2. On the SAT screen, type `status trunk` *group/member*.

   A display screen similar to the status station screen displays the trunk information.

Legal wiretapping

You can administer Service Observing permissions to a selected target endpoint. Use this option if you receive a court order to provide law enforcement access to certain calls placed to or from an IP endpoint. Put the observer and the target endpoint in a unique Class of Restriction (COR) with the same properties and calling permissions as the original COR. Without this configuration, the target user might know of the change.

For more information about Service Observing, see Table 7: Media Encryption interactions on page 114

Possible failure conditions

Because of restricted media capabilities, using Media Encryption in combination with an administered security policy might lead to blocked calls or call reconfigurations. For example, consider that the IP codec set used between two network regions is administered as aes or aea. If a call between two endpoints does not support at least one common encryption option, then a voice path is unavailable.

Interactions of media encryption with other features

Media Encryption does not affect most Communication Manager features or adjuncts, except for those listed in Table 7: Media Encryption interactions on page 114

Table 7: Media Encryption interactions

Interaction	Description
Service Observing	You can Service Observe a conversation between encrypted endpoints. The conversation remains encrypted to all outside parties except the communicants and the observer.
Voice Messaging	Any call from an encryption-enabled endpoint is decrypted before it is sent to a voice messaging system. When the G4xx Media Gateway and Avaya Aura® Media Server receives the encrypted voice stream, Media Processor decrypts the packets before sending them to the voice messaging system. The voice messaging system then stores the packets in unencrypted mode.
Hairpinning	Hairpinning is not supported when one or both media streams are encrypted, and Communication Manager does not request hairpinning on these encrypted connections.
VPN	Media encryption complements virtual private network (VPN) security mechanisms. Encrypted voice packets can pass through VPN tunnels, essentially double-encrypting the conversation for the VPN leg of the call path.

Table continues…

Interaction	Description
H.323 trunks	Media Encryption on a call varies based on the following conditions at call set up: • Whether shuffled audio connections are permitted. • Whether the call is an interregion call. • Whether IP trunk calling is encrypted or not. • Whether the IP endpoint supports encryption. • The media encryption setting for the affected IP codec sets. These conditions also affect the codec set that is available for negotiation each time a call is set up. T.38 packets can be carried on an H.323 trunk that is encrypted. However, the T.38 packet is sent in the clear.

Network recovery and survivability

Various options are available to ensure quick network recovery and survivability. This section discusses the following features and options:

- Network management
- H.248 link loss recovery
- Survivable core servers
- QoS policies
- Monitor network performance

Network management

Network management is the practice of using specialized software tools to monitor and maintain network components. Proper network management is a key component for the high availability of data networks.

The two basic network management models are:

- Distributed: Specialized, nonintegrated tools to manage discrete components.
- Centralized: Integrated network management tools and organizations for a more coherent management strategy.

This section describes Avaya VoIP Monitoring Manager and Avaya Policy Manager, which are integrated management tools.

For a detailed discussion of network management products from Avaya, common third-party tools, and the distributed and centralized management models, see *Avaya Aura® Core Solution Description*.

Monitor network performance

Using the Avaya VoIP Monitoring Manager, a VoIP network quality monitoring tool, you can monitor the following quality-affecting network factors:

- Jitter levels
- Packet loss
- Delay
- Codecs used
- RSVP status

QoS policies

Avaya Policy Manager is a network management tool for controlling Quality of Service (QoS) policies for both the data and the voice networks.

QoS policies are assigned according to network regions and are distributed through the Enterprise Directory Gateway to your systems and to routers and switching devices.

In Figure 12: Avaya Policy Manager application sequence on page 116, you can see how Avaya Policy Manager works.

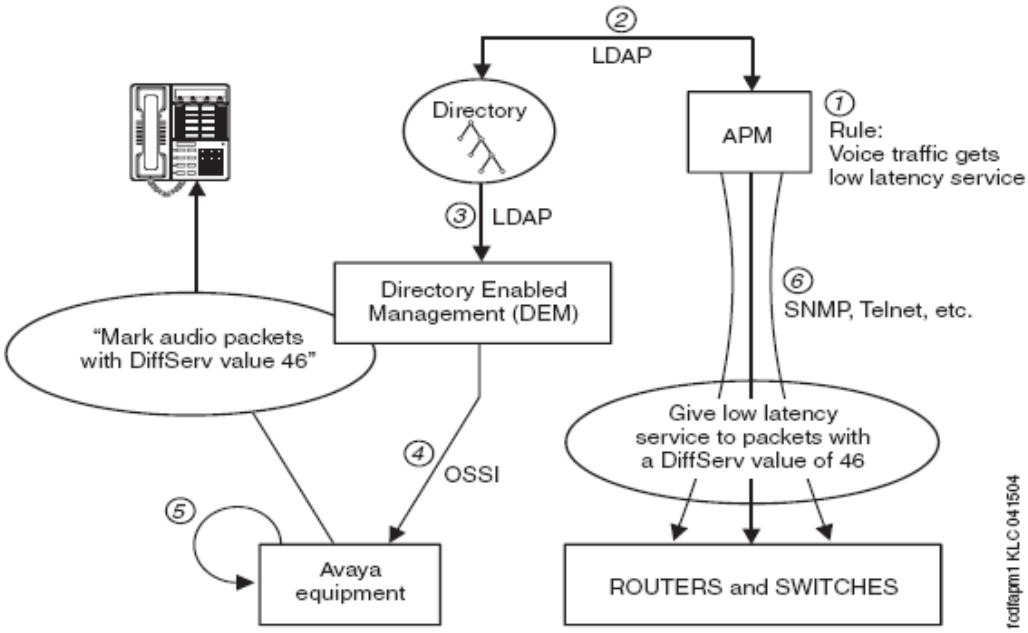


Figure 12: Avaya Policy Manager application sequence

First, business rules are established in Avaya Policy Manager. Avaya Policy Manager uses LDAP to update Communication Manager. Directory Enabled Management (DEM) identifies the change in the directory. EDG updates Communication Manager administration through the Ethernet switch. Using messages from the Communication Manager, PROCR, G4xx Media Gateway, Avaya Aura® Media Server, and IP phones mark audio packets with DSCP as 46. Avaya Policy

Manager then distributes policy information to other network devices, including low latency service for DiffServ value of 46.

For more information about Avaya Policy Manager, go to the Avaya Support website at http://support.avaya.com.

H.248 link loss recovery

H.248 Link Loss Recovery is an automated way in which the gateway reacquires the H.248 link. H.248 Link Loss Recovery can occur when the link is lost from either a primary call controller or a survivable remote server. The H.248 link between a server running Communication Manager and a gateway, and the H.323 link between a gateway and an H.323-compliant IP endpoint, provide the signaling protocol for:

- Call setup
- Call control with user actions such as Hold, Conference, or Transfer, while the call is in progress
- Call tear-down

If the link is out of service, Link Recovery preserves any existing calls and attempts to reestablish the original link. If the gateway or endpoint cannot reconnect to the original server or gateway, Link Recovery automatically attempts to connect with alternate survivable processor.

Overlap with the Auto Fallback to Primary feature occurs when:

- Link Loss Recovery starts while the gateway tries to migrate back to the primary.
- Link Loss Recovery new registration message indicates that service is being obtained from elsewhere.

A rare condition can exist in which an outstanding gateway registration to the primary exists while the link to the survivable remote server is lost. The gateway awaits a denial or acceptance from the primary call controller. If the call controller accepts, then Link Loss Recovery is terminated, and the gateway is serviced by the primary call controller. If the call controller denies, then the gateway immediately sends a new registration to the primary call controller. The registration indicates no service, and the existing H.248 Link Loss Recovery feature takes over.

Both features try to return service to the primary call controller. However, Link Loss Recovery returns service based on a link failure, whereas auto fallback to primary returns service based on a working fragmented network.

Auto fallback to primary controller for branch gateways

The auto fallback to primary controller feature automatically returns a fragmented network, in which a number of Branch Gateways are being serviced by one or more survivable remote servers, to the primary server. This feature is targeted towards all Branch Gateways. By migrating the gateways back to the primary automatically, the distributed telephony switch network can be made whole sooner without human intervention.

The auto fallback migration, in combination with the connection preservation feature for H.248 gateways is connection preserving. Stable connections are preserved, while unstable connections,

such as ringing calls, are not preserved. A very short interval without dial tone can still exist for new calls.

The gateway presents a new registration parameter that indicates that Service is being obtained from a survivable remote server. The parameter indicates the number of active user calls on the gateway platform. The server administers each gateway with a set of rules for Time of Day migration, enable or disable, and the setting of call threshold rules for migration.

Using this feature, the administrator can define any of the following rules for migration:

- The gateway must migrate to the primary automatically or not.
- The gateway must migrate immediately when possible, regardless of active call count.
- The gateway must only migrate if the active call count is 0.
- The gateway must only migrate within a window of opportunity by providing day of the week and time intervals per day. This option does not take call count into consideration.
- The gateway should be migrated within a window of opportunity by providing day of the week and time of day, or immediately if the call count reaches 0. Both rules are active at the same time.

Internally, the primary call controller gives priority to registration requests from the gateways that are currently not being serviced by an survivable remote server. This priority is not administrable.

An auto-fallback can be denied for several reasons, which can result from general system performance requirements or from administrator-imposed requirements. General system performance requirements can include denial of registration because of too many simultaneous gateway registration requests.

Administrator-imposed requirements for denial of a registration can include:

- Registrations restricted to a windowed time of day.
- Migration restricted to a condition of 0 active calls, that is, there are no users on calls within the gateway in question.
- The administered minimum time for network stability has not been exceeded.

This feature does not preclude an older gateway firmware release from working with Communication Manager 10.x or vice versa. However, the auto-fallback feature is not available.

For this feature to work, the call controller is required to have Communication Manager, while the gateway is required to have the gateway firmware available at the time of the Communication Manager 10.x release.

Existing branch gateways are the targets.

For each gateway, the following administration must be performed:

- Adding Recovery Rule to Gateway screen.
- Scheduling the auto fallback within the system-parameters area on the System Media Parameters Gateway Automatic Recovery Rule screens.

Basic feature operation

This sections shows the basic operation of the auto fallback to primary for branch gateways feature. By default, this feature is disabled in the gateway or server.

If the gateway is initially registered with an older server, the gateway uses the version information exchange to prevent fallback to the primary automatically.

- By administering this feature on a server, this feature can be enabled for any or all gateways controlled by the server.

  The enable or disable administration on the server determines whether the server accepts or denies registration requests. The requests are sent with a parameter that service is being obtained from a survivable remote server. However, the gateway continuously attempts to register with the server, even if the server has been administered never to accept the registration request. When the auto fallback feature is disabled on the server, the server is administered to never accept registration requests. Then, a manual return of the gateway is required, which generates a different registration message that is accepted by the server.

  Note:

  The registration messages are still valuable when auto fallback is disabled on the server. Because registration messages function as keep-alive messages, these messages can be used to monitor the stability of the network over time.

- The permission-based rules that include time of day and context information are only available with the server.

  The survivable remote server does not require any of these translations.

- When associated with a primary controller running Communication Manager, the gateway attempts to register with the primary controller when connected to a survivable remote server.

  This registration attempt happens every 30 seconds after the gateway can communicate with the primary controller. The registration message contains an element that indicates that a survivable remote server is servicing the gateway. The message also contains the number of active user calls on that gateway.

- On the initial registration request, the primary controller starts the encrypted TCP link for H.248 messaging.

  The TCP link is started for H.248 messaging regardless of whether that initial registration is successful. The encryption is maintained throughout the period when the registration requests are valid. The encryption is also maintained after a registration is accepted by the primary controller. Encryption of the signaling link is performed at the outset during this automatic fallback process. The encryption ensures the security of the communication between the primary call controller and the gateway.

- The primary controller, based on the administered rules, can allow or deny a registration.

  If the primary controller gets a registration message without Service State information, then the primary honors those registration requests above all others immediately. Registration messages can originate without Service State information, for example, from an older gateway, or when a new gateway is without service.

- If registration is denied, the gateway continues to send the registration message every 30 seconds, which acts as a de facto keep-alive message.
- The gateway constantly monitors the call count on the platform and asynchronously sends a registration message when 0 context is achieved.
- After the registration message is accepted by the primary, the H.248 link to the survivable remote server is dropped.

Older gateway loads

The auto fallback feature on the server is passive in nature. An older gateway load trying to register with the current Communication Manager load registers with priority. The prioritization occurs because the value of the Service-State is that of a gateway without service. Defined rules for the gateway are ignored because an older gateway firmware release attempts registration only when no other server services the gateway. Therefore, the administration of rules for old gateway firmware loads are irrelevant.

Adding Recovery Rule to the Media Gateway screen

Procedure

1. On the SAT screen, type `change media-gateway` *n*, where *n* is the assigned media gateway number, and press `Enter`.

   The system displays the Media Gateway screen.

2. In the **Recovery Rule** field, type one of the following recovery rule number:

   - None is the default value, which indicates that automatic fallback registrations are not accepted.
   - A value between 1 to 50, or 1 to 999 applies a specific recovery rule to that numbered gateway.

   S8300E support up to 50 gateways, and a standalone server supports up to 999 gateways.

   Note:

   A single recovery rule number can be applied to all gateways, or each gateway can have a recovery rule number or any combination in between.

   By associating the recovery rule to the Media Gateway screen, an administrator can use the **`list media-gateway`** command to see which gateways have the same recovery rules. All administration parameters for the gateways are consolidated on a single screen. The actual logic of the recovery rule is separate, but an administrator can start from the Gateway screen and proceed to find the recovery rule. These changes also apply to the **`display media-gateway`** command.

   For more information about the fields on this screen, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers* at http://support.avaya.com.

System Parameters Media Gateway Automatic Recovery Rule screen

You can define recovery rules on the System Parameters Media Gateway Automatic Recovery Rule screen. You can access this screen by using the **`change system-parameters mg-recovery-rule`** *n* command. This screen is available within the system-parameters area of administration screens. The maximum number of screens that can be administered correspond to the maximum number of gateways supported by the server. For the S8300E, you can administer up to 50 screens, while for standalone servers, you can administer up to 999 screens.

System Parameters Media Gateway Automatic Recovery Rule field descriptions

Name	Description
Recovery Rule Number	The number of the recovery rule: • Up to 50 for the S8300E server • Up to 999 for the standalone servers
Rule Name	Optional text name for the rule to aid in associating rules with gateways.
Migrate H.248 MG to primary	Administrable options for migrating the H.248 media gateway to primary: • immediately • 0-active calls • Time-day-window • Time-window-OR-0-active-calls For more information about these options, see Migrate H.248 MG to primary options.
Minimum time of network stability	Administrable time interval for stability in the H.248 link before auto fallback can happen. Enter a value between 3 and 15 minutes. The default value is 3 minutes.

Migrate H.248 MG to primary options

The following options are available for the Migrate H.248 MG to primary field:

- immediately: The first gateway registration that comes from the gateway is honored, regardless of context count or time of day.

  A warning is visible when a user selects this option. This option is the default value for all rules.

- 0-active calls: The first gateway registration reporting 0 active calls is honored.
- Time-day-window: A valid registration message received during any part of this interval is honored.

Note:

Time of day is local to the gateway.

Any number of active calls are supported. The time scale provided for each day of the week goes from 00 to 2300 hours (military time). The user must type an x or X for each hour where return migration must be permitted. To disallow return migration for a given hour, the field is left blank. This method gets around overlapping time issues between days of the week. Users can specify as many intervals as required.

- Time-window-OR-0-active-calls: A valid registration is accepted anytime, when a 0 active call count is reported. The registration is also accepted if a valid registration with any call count is received during the specified time or day intervals.

  The time scale provided for each day of the week goes from 00 to 2300 hours (military time). The user must type an x or X for each hour where return migration must be permitted. To disallow return migration for a particular hour, the field is left blank. This method gets around overlapping time issues between days of the week. Users can specify as many intervals as required.

Recovery rules applied across all gateways

Administrators can see how the recovery rules are applied across all gateways from the Media Gateway Report screen. Use the **`list media-gateway`** command to view the recovery rule for each gateway in the network.

```
list media-gateway                                        Page 1 of 1
                          MEDIA GATEWAY REPORT

Num  Name                  Serial No/       IP Address/     Type  NetRgn/   Reg?
                           FW Ver/HW Vint   Cntrl IP Addr          RecRule

1    GW#1 Boxster Lab      01DR11131345     135.8  .77 .62  g700   1        n
                           unavailable                              none

2    MG2 Boxster MV Lab    02DR06750093                      g700   1        n
                           unavailable                              10

3    MG3 Boxster MV Lab    01DR10245104     135.8  .77 .68  g700   1        n
                           unavailable                              none
```

Figure 13: Media Gateway Report screen

In this example, check the values administered for gateways 1 and 3. With the administered values, the primary controller rejects registration requests when the gateway is active on a survivable remote server. Gateway 2, on the other hand, is administered with Recovery Rule number 10. Use the **`display system-parameters mg-recovery-rule`** 10 command to view the details of recovery rule number 10.

Chapter 5: 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. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.

3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.

- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite 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 collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.

- Send feedback for a topic.

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
70380W	What's New with Avaya Aura® 10.2
70390W	Upgrading to Avaya Aura® 10.2
70410W	Migrating to ASP R6.0.x (KVM on RHEL 8.10) Hypervisor
71301V	Integrating Avaya Aura® Communications Applications
72301V	Supporting Avaya Aura® Communications Applications
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

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 **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select 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. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

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

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W