Administering Network Connectivity on Avaya Aura® Communication Manager

Release 7.0.1
555-233-504
Issue 2
May 2016

© 2015-2016, Avaya, Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License type(s)

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

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

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number

indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see

the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya and Avaya Aura® are registered trademarks of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 9
Purpose 9
Change history 9
Warranty 10
Chapter 2: Networking Overview 11
Network terminology 11
Digital telephone calls 11
Network regions 12
Features affected by the increase in locations and network regions 14
Interswitch trunk connections 15
IP-connected networks 15
Branch office networks 15
Control networks 16
Spanning Tree Protocol 16
Inter-Gateway Alternate Routing 16
Dial Plan Transparency 17
Network quality management 18
VoIP transmission hardware 18
Processor Ethernet 19
LAN security 21
Connection Preservation 22
Session refresh handling 22
Connection Preserving Migration 23
Chapter 3: Port network configurations 25
IP port network connectivity 25
Reliability 25
Simplex server 26
Duplex server 26
Simplex IP-PNC for the single control network 27
Architecture of simplex server IP-PNC 28
Duplicated TN2602AP circuit packs in IP-PNC port networks 29
Circuit packs for duplicated bearer connections 30
Duplex IP-PNC (single control network) 30
Architecture of duplex IP-PNC single control network 32
Duplex server IP-PNC for a duplicated control network 34
Architecture of duplex IP-PNC duplicated control network 34
Duplex server IP-PNC for a duplicated control and bearer network connection 36
Architecture of duplex IP-PNC duplicated control and duplicated bearer network 37
Example of IP-PNC port networks with different reliability levels 39

Chapter 4: Converged Networks 42
Voice over IP converged networks 42
Network assessment 42
VoIP hardware 43
Universal DS1 circuit packs and MM710 T1/E1Media Module 43
TN799DP Control LAN 46
TN2302AP IP Media Processor 50
TN2602AP IP Media Resource 320 51
TN2312BP IP Server Interface 54
MM760 VoIP Media Module 58
Avaya gateways 59
Avaya Aura® Media Server 60
IP trunks 60
SIP trunks 60
Creating a SIP trunk signaling group 61
H.323 trunks 62
Preparing to administer H.323 trunks 62
Verifying customer options for H.323 trunking 63
Administering C-LAN and IP Media Processor circuit packs for simplex/duplex servers 63
QoS parameters 64
IP node names and IP addresses 64
Assigning IP node names 65
Defining IP interfaces 66
Defining IP interfaces for duplicated TN2602AP 66
Best Service Routing 66
Administering an H.323 trunk 67
H.323 trunk signaling group 67
Creating an H.323 trunk signaling group 68
Creating a trunk group for H.323 trunks 70
Modifying the H.323 trunk signaling group 72
Dynamic generation of private/public calling party numbers 72
Avaya IP phones 74
IP softphones 74
Avaya IP telephones 77
Hairpinning, shuffling, and direct media 81
Examples of shuffling 83
Hairpinning and shuffling administration interdependencies 89
Network Address Translation 91
Hairpinning and shuffling 94
Fax, modem, TTY, H.323 Clear Channel calls over H.323 IP trunks, and SIP 64K Data calls over SIP trunks 99
Relay 100
Pass-through 100

T.38 ... 101
V.150.1 Modem Relay ... 101
SIP 64K Data ... 102
Administering fax, TTY, modem, and clear-channel calls over IP trunks ... 102
Considerations for administering FAX, TTY, modem, and Clear-Channel transmission ... 103
FAX, TTY, modem, and clear channel transmission modes and speeds ... 105
Bandwidth for FAX, modem, TTY, and clear channel calls over IP networks ... 109
Media encryption for FAX, modem, TTY, and clear channel ... 110
SRTP media encryption ... 112
Platforms ... 113
Administering SRTP ... 113
Administering SRTP for video signaling ... 114
Chapter 5: Voice, Video, and Network quality administration ... 116
Factors causing voice degradation ... 116
Packet delay and loss ... 117
Echo ... 118
Transcoding ... 121
Bandwidth ... 122
Quality of Service and voice quality administration ... 122
Layer 3 QoS ... 123
Layer 2 QoS ... 123
IP codec sets ... 125
IP network regions ... 128
Call Admission Control ... 133
Administering DPT ... 137
Network Region Wizard ... 138
Manually interconnecting the network regions ... 139
Setting network performance thresholds ... 144
Enabling or disabling spanning tree ... 145
Jitter buffers ... 146
UDP ports ... 146
Media encryption ... 147
Limitations of media encryption ... 147
Types of media encryption ... 147
License file ... 148
Legal wiretapping ... 151
Possible failure conditions ... 152
Interactions of media encryption with other features ... 152
Network recovery and survivability ... 153
Network management ... 153
H.248 link loss recovery ... 154
Administrable IPSI Socket Sanity Timeout ... 161
Survivable core servers ... 163

Improved port network recovery from control network outages..... 164
Port Network Recovery Rules screen field descriptions..... 165
Survivability..... 166
Chapter 6: Resources..... 167
Documentation..... 167
Finding documents on the Avaya Support website..... 168
Training..... 169
Viewing Avaya Mentor videos..... 170
Support..... 170
Appendix A: PCN and PSN notifications..... 171
PCN and PSN notifications..... 171
Viewing PCNs and PSNs..... 171
Signing up for PCNs and PSNs..... 172

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 Partners

Change history

Issue	Date	Summary of changes
1.0	August 2015	Initial release
2.0	May 2016	• Updated the Administering an IP Codec set on page 126 section to add information about OPUS Codec bit-rate options. • Updated the Network regions on page 12 section to add information about Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9 common servers.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com under **Help & Policies> Policies & Legal > Warranty and Product Lifecycle**. See also **Help & Policies > Policies & Legal > License Terms**.

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 nontelephony 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

- Distributed Communications System (DCS) signaling data

Use DCS to configure two or more communication switches as a single switch. DCS provides attendant features and voice terminal features between these switch locations. DCS simplifies dialing procedures and ensures transparent use of some Communication Manager features. Feature transparency means that features are available to all users on DCS regardless of the switch location.

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 C-LANs, MedPros, gateways, or other 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. This increase in the number of network regions and locations applies to customers that use Communication Manager installed on the following servers and VMware platforms:

- HP ProLiant DL360 G7
- HP ProLiant DL360 G9
- Dell™ PowerEdge™ R610
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630

With the increase in the number of network regions and locations that Communication Manager supports, organizations can expand businesses to various locations globally. Organizations can also efficiently manage bandwidth by allocating the required bandwidth between a pair of network regions.

To support the increase to 2000 network regions and locations, 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 13. 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.

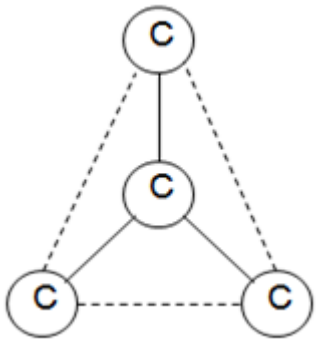


Figure 1: Core network regions

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 13.

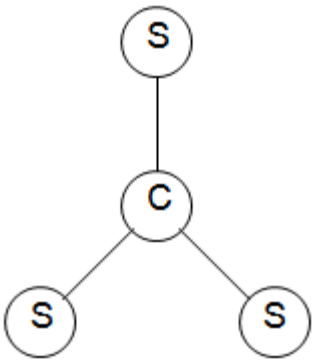


Figure 2: Core and stub network regions

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 14

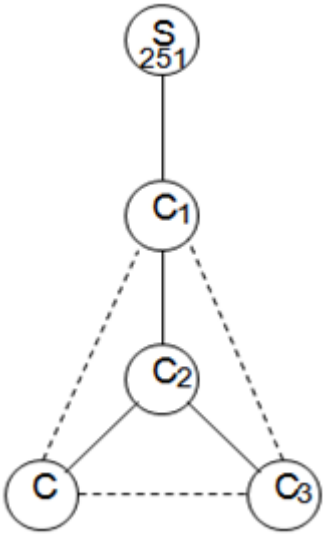


Figure 3: Communication Pathway from a stub network region to a core network region

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.

You must assign all Communication Manager hardware, such as branch gateways, media processors, C-LANs, and G650 cabinets to network regions 1 to 250. This assignment must be done regardless of whether the network region is a core network region or a stub network region.

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.

IP-connected networks

For more information about IP-connected (IP-PNC) networks, see Chapter 3: Port network configurations on page 25.

Branch office networks

In Communication Manager environments, MultiVOIP™ gateways provide distributed networking capabilities to small branch offices of large corporations. MultiVOIP extends the call features of a centralized Avaya server. MultiVOIP provides local office survivability to branch offices of up to 15 users who use analog or IP telephones.

For more information about MultiVOIP™ gateways, go to http://www.multitech.com/PARTNERS/Alliances/Avaya/.

Control networks

Control networks are networks over which Communication Manager exchanges signaling data with port networks. Communication Manager exchanges signaling data through the IPSI circuit packs.

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 intergateway 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 interregion voice bearer connection when the following five conditions are met:

- An intergateway 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 Home SES.
- 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 137.

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 116
- *Avaya Aura® Solution Design Considerations and Guidelines*, 03-603978.

VoIP transmission hardware

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

- TN799DP control LAN (C-LAN) interface

Provides TCP/IP connectivity over Ethernet between servers and gateways, or Point to Point Protocol (PPP) between servers and adjuncts.

- TN2312BP IP Server Interface (IPSI)

  Transports control messages between servers and port networks.

- TN2302AP IP Media Processor and TN2602AP IP Media Resource 320

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

- 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 S8300D Server and S8300E.
  - Survivable Remote server backup for a remote server.

  The branch gateways include the G700, G250 Branch Gateway, G350 Branch Gateway, G430 Branch Gateway G450 Branch Gateway and IG550.

  Note:

  S8300E supports G430 Branch Gateway and G450 Branch Gateway.

- MM760 VoIP Media Module

  Provides another 64 VoIP channel in the G700 motherboard VoIP engine. The MM760 VoIP Media Module is a clone of the G700.

- Avaya Aura® Media Server

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

For more information about Avaya hardware devices, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

For information about the administration tasks for this equipment, see VoIP hardware on page 43.

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*, 03-300509.

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`.

In Communication Manager Release 5.2 and later, 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 and port networks on a Survivable Core server

In Communication Manager Release 5.2 and later, the capabilities of survivable core servers are enhanced to support the connection of IP devices to the Processor Ethernet (PE) interface and to C-LAN interfaces. C-LAN interfaces are located in G650 gateways. G650 are port networks.

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 optionally control port networks through IPSI simultaneously. Without port networks in the configuration, 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 the C-LAN on the main server, the C-LAN must have IP connectivity to the LAN. The LAN must be assigned to the NIC used for PE on the survivable core 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:

- 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 C-LAN 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 21 shows a high-level switch schematic with a TN799 (C-LAN) circuit pack.

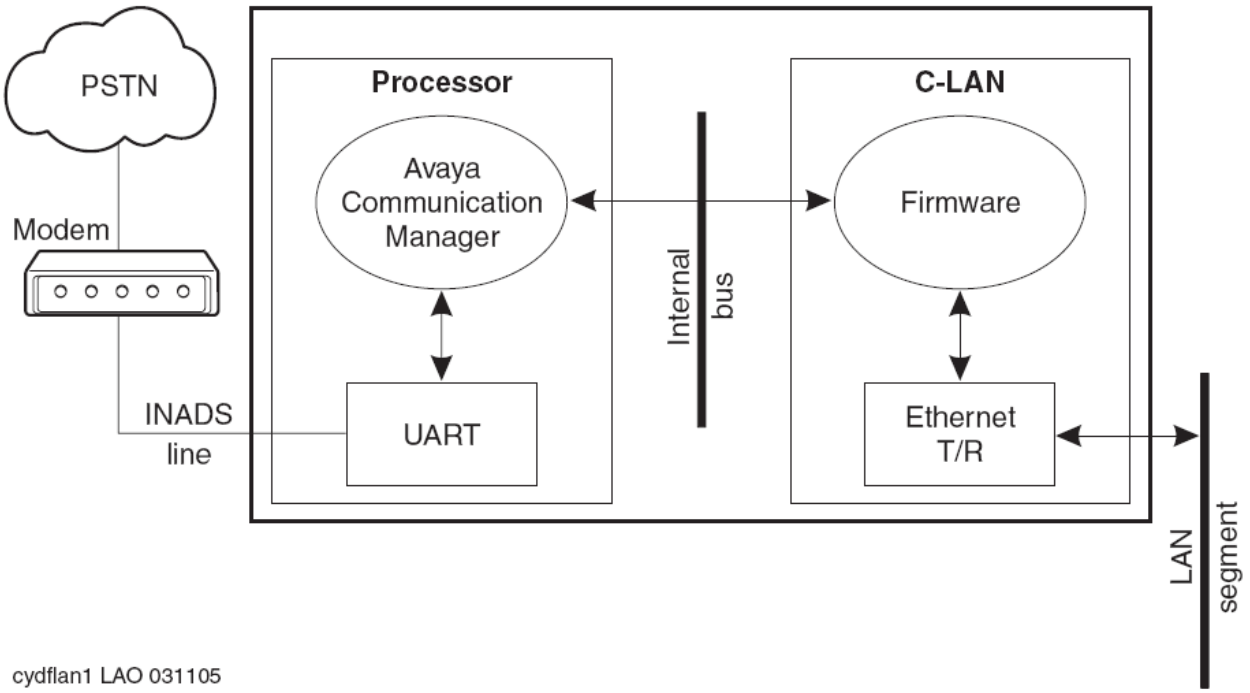


Figure 4: Security-related system architecture

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 C-LAN firmware.

  The user can only enter SAT commands that request C-LAN information or configure C-LAN connections.

- Communication Manager disables the C-LAN application TFTP and cannot enable the application.

  TELNET only interconnects C-LAN 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 (C-LAN) 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*, 555-245-207.

Note:

The survivable remote server is also known as Enhanced Local Survivability (ELS).

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.

Chapter 3: Port network configurations

You can control call processing of port networks in various ways by using Communication Manager. Using only Ethernet connections, you can establish control networks. Over LAN/WAN connections, you can transmit voice, fax, and TTY. Types of reliability achieved with Duplex servers can include single control and bearer networks, duplicated control networks, duplicated control and bearer networks, or a combination of reliabilities.

Types of control networks and the corresponding types of reliability:

- Single control and bearer networks are standard reliability.
- Duplicated control networks are high reliability.
- Duplicated control and bearer networks are critical reliability.

IP port network connectivity

IP port network connectivity allows servers and port networks and Branch Gateways to be connected over IP networks. Communication Manager uses a proprietary method to package signaling messages over IP. This method allows deployment of communications systems throughout a customer's data network.

For bearer transmission and control signaling from the server, IP port network connectivity (IP-PNC) uses LAN or WAN connections between port networks. Each port network must have either one or two control IPSI circuit packs for control signaling.

Reliability

Reliability is the capability of a Communication Manager configuration to maintain service when components within the configuration fail. Components that fail might include Ethernet switches, circuit packs, or gateways. The available reliability levels depend on whether the port networks use IP-PNC and whether the server is simplex or duplex.

Simplex server

A Simplex server provides several reliability options.

- Standard reliability:

  For IP port network connectivity (IP-PNC), a Simplex server supports a single IPSI for controlling the IP-PNC port network, TN2302BP, or TN2602AP circuit packs. The circuit packs are used for the bearer network. However, TN2602AP circuit packs are implemented in the load-balancing mode only.
- Duplicated bearer reliability:

  For IP-PNC, a Simplex server does not support duplicated control. However, IP-PNC port networks can have duplicated TN2602AP circuit packs to duplicate the bearer connections. In a port network with duplicated TN2602AP circuit packs, control signaling always occurs over a direct IPSI connection to the server. A duplicated bearer network that uses TN2602AP circuit packs is implemented for each port network. Uniform implementation for all port networks within the configuration is not required.

Duplex server

A Duplex server has multiple levels of reliability.

IP port network connectivity

Reliability for Port Networks that use IP port network connectivity (IP-PNC) within a single Communication Manager configuration is implemented for each Port Network. Uniform implementation for other IP-PNC Port Networks within the configuration is not required. In addition, duplicated bearer and duplicated control can be implemented independently of each other.

An IP-PNC Port Network can have one of the following reliability levels:

- Standard duplicated servers:

  A single IPSI provides control signaling between the Port Network and the server. The Port Network contains only single or load balancing TN2302BP, or TN2602AP circuit pack pairs. check data accuracy
- Duplicated control:

  In addition to the standard duplicated servers, duplicated IPSIs for control reside in each Port Network. The Port Network contains only single or load balancing TN2302BP, or TN2602AP circuit pack pairs.
- Single control and duplicated bearer:

  In addition to the standard duplicated servers, duplicated TN2602AP circuit packs reside in each Port Network to provide duplicated bearer.

  Note:

  For duplicated bearer for IP-PNC Port Networks, use duplicated IPSI control.
- Duplicated control and bearer:

In addition to the standard duplicated servers, duplicated IPSIs for control reside in each Port Network. Duplicated TN2602AP circuit packs reside in each Port Network to provide duplicated bearer.

Simplex IP-PNC for the single control network

In the IP-PNC configuration, the Simplex server uses IP connections to control call processing on the port networks. The Simplex server uses an existing VoIP-ready IP infrastructure to send voice between port networks over the IP network. With this solution, customers save the cost of building a separate telephony network. In this type of configuration, all port networks are connected to the server and to each other over the customer network. You can configure up to 64 port networks in an IP-PNC configuration. Depending on the Ethernet switches to connect to the port networks and the port network locations, the network can require multiple Ethernet switches to support the port networks.

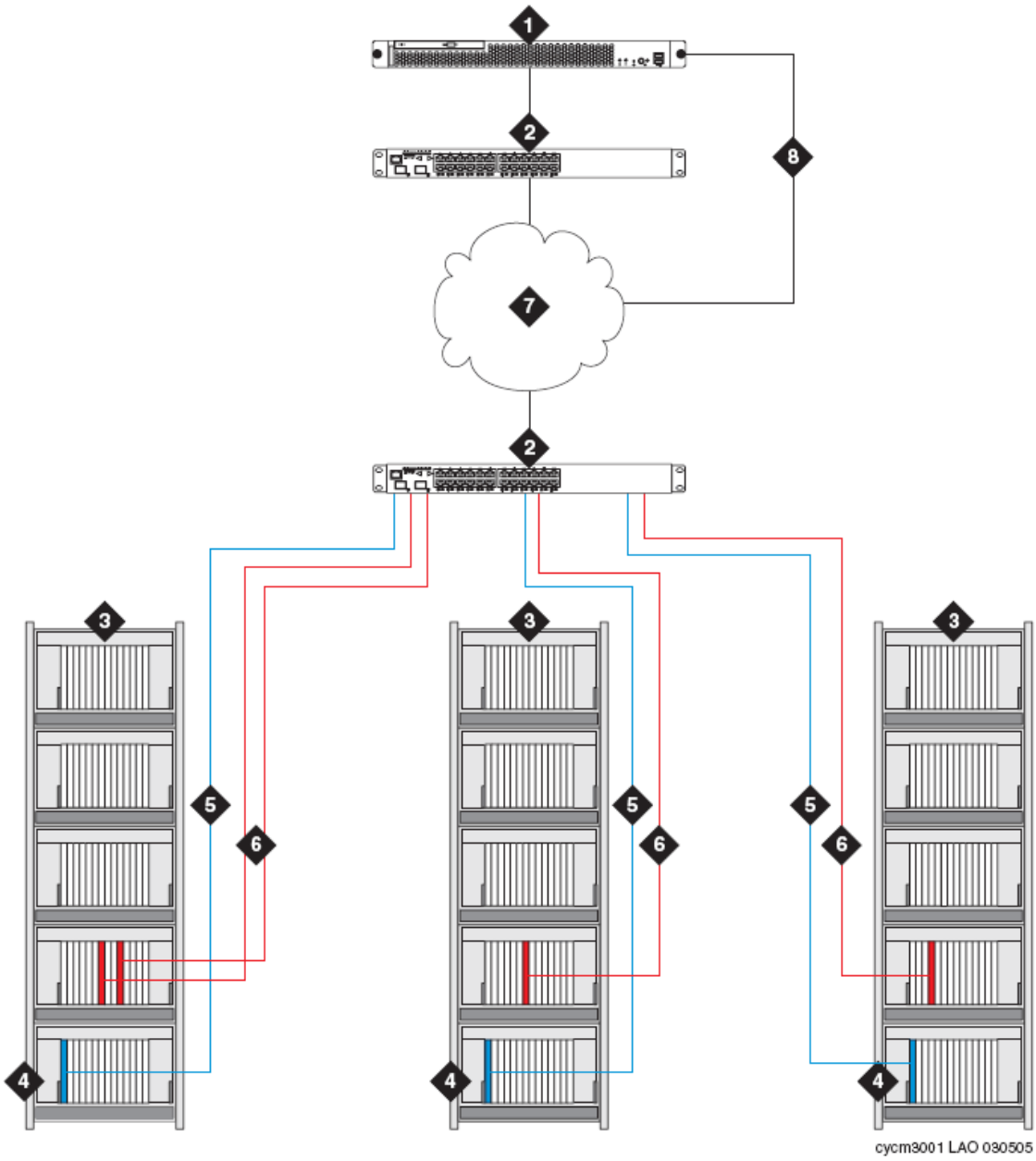
G650 Media Gateway: You can use G650 Media Gateway in an IP-PNC network. A G650 port network can consist of one to five G650 gateways in a stack connected by a TDM or LAN bus cable. One gateway that functions as a control gateway in position A at the bottom of the stack contains the TN2312BP IPSI circuit pack. Only G650 Media Gateway is available for new installations. However, different migrations from older systems are supported.

IP/TDM conversion resource: Each port network must contain at least one TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 circuit pack. The TN2302AP or TN2602AP circuit pack provides IP-TDM voice processing for endpoint connections between port networks. You can insert the circuit packs in any gateway in the port network. Each port network can optionally house a TN799DP C-LAN circuit pack for control of the:

- G150 Branch Gateway
- G700, G450, G430, G350, and G250 Branch Gateways
- IP endpoints
- Adjunct systems, such as messaging and firmware downloads

Ethernet connections: In the IP-PNC configuration, the Simplex server connects to the gateways through a single Ethernet switch. Each port network connects to the Simplex server through a local Ethernet switch. As a result, remote port networks in an IP-PNC configuration over WAN can require Ethernet switches in addition to the Ethernet switch that supports the Simplex server. You can administer IP connections to the Simplex server as dedicated private LAN connections or connections over the customer LAN.

Architecture of simplex server IP-PNC



Number	Description
1	Simplex server C or B.
2	Ethernet Switch.

Table continues…

Number	Description
	For local LAN connections, the same Ethernet switch can connect both the servers and the gateways. For remote LAN/WAN connections, the remote gateways must have an Ethernet switch at the remote location.
3	Port networks (G650 Media Gateway or stack).
4	Port network control gateway in the A position in the gateway stack which contains TN2312AP/BP IPSI circuit pack for IP connection to server. • A TN2312AP/BP IPSI circuit pack for IP connection to server. **Note:** For the G650 Media Gateway, you require the BP version of the TN2312 to provide environmental maintenance.
5	IPSI-to-server control network connection via Ethernet switch.
6	LAN connections of TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 for IP-TDM voice processing and optional TN799DP C-LAN for control of IP endpoints **Note:** The number of TN2302AP, TN2602AP, and TN799DP circuit packs varies, depending on the number of IP endpoints, port networks, and adjunct systems. These circuit packs can be inserted into a port gateway (shown in figure) or the port network control gateway.
7	Customer LAN/WAN.
8	LAN connections of servers for remote administration.

Duplicated TN2602AP circuit packs in IP-PNC port networks

For a simplex server, any IP-PNC port network can contain load-balancing or duplicated TN2602AP circuit packs. However, TN2602AP circuit packs do not need to be implemented uniformly within the system. Port networks can either have a single TN2602AP circuit pack, load-balancing TN2602AP circuit packs, or duplicated TN2602AP circuit packs. A simplex server can have duplicated bearer connections although the server does not support a duplicated control network.

Circuit packs for duplicated bearer connections

For a simplex server, each IP-PNC can contain load-balancing circuit packs, duplicated TN2602AP circuit packs, or load-balancing TN2302AP circuit packs.

Port networks can have one of the following circuit packs:

- A TN2302AP circuit pack
- A TN2602AP circuit pack
- A combination of TN2302AP and TN2602AP circuit packs
- Load-balancing TN2302AP circuit packs
- Load-balancing TN2602AP circuit packs
- Duplicated TN2602AP circuit packs

A simplex server can have duplicated bearer connections even if the server does not support a duplicated control network.

Duplex IP-PNC (single control network)

In this configuration, the duplex servers connect to one or more port networks over an Ethernet connection using an interim Ethernet switch and a dedicated LAN connection or the customer LAN. Each port network is connected to the Ethernet switch or LAN with a CAT5 cable through a TN2312AP/BP IP Server Interface (IPSI) card.

With this solution, customers save the cost of building a separate telephony network. In this configuration, all port networks are connected to the customer network and call control from the duplex server is also sent over the customer network. You can configure upto 64 port networks in an IP-PNC configuration.

Only the G650 Media Gateway is available for new installations. However, because different migrations from older systems are supported, an IP-PNC network supports the G650 Media Gateway. A G650 port network can consist of one to five G650 gateways in a stack connected by a TDM/LAN bus cable. A control gateway in position A at the bottom of the stack contains a TN2312BP IPSI circuit pack.

IP/TDM conversion resource:

Each port network must contain at least one TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 circuit pack. The TN2302AP or TN2602AP circuit pack provides IP-TDM voice processing of endpoint connections between port networks. Optionally, one or more TN799DP C-LAN circuit packs can be present for controlling:

- the G150, G700, G450, G430, G350, and G250 branch gateways
- IP endpoints

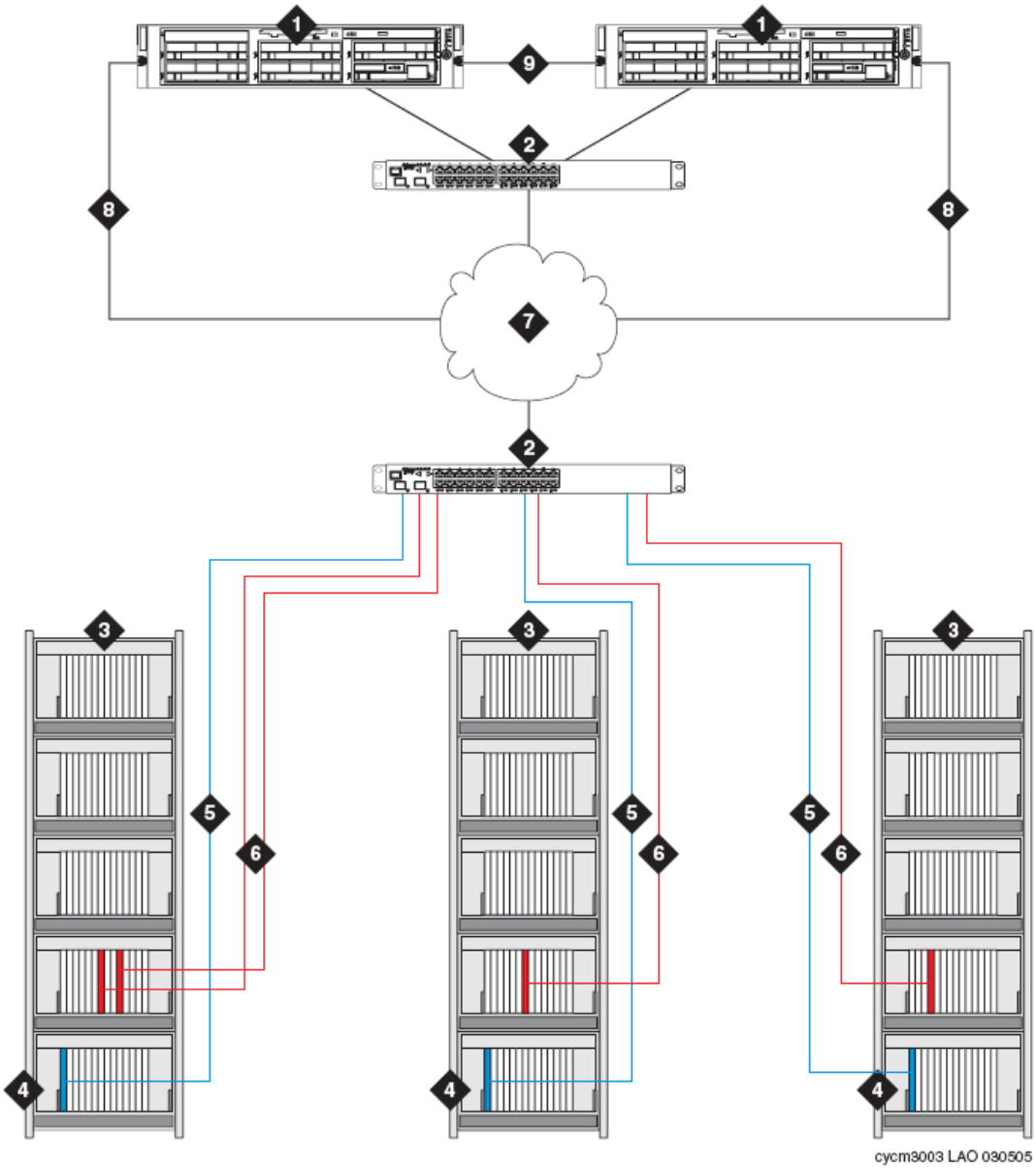
- adjunct systems such as messaging
- firmware downloads

These circuit packs can be inserted in any gateway in the port network.

Ethernet connections:

In the IP-PNC configuration, the duplex server connects to the gateways through a single Ethernet switch. Each port network also has a connection to the network or the duplex server through a local Ethernet switch. Therefore, remote port networks in an IP-PNC configuration over a WAN, which normally requires routers to complete the connection, require dedicated Ethernet switches. These Ethernet switches are in addition to the Ethernet switch that supports the duplex server. IP connections to the duplex server are administered as dedicated private LAN connections or connections over the customer LAN.

Architecture of duplex IP-PNC single control network



Number	Description
1	Duplex server.
2	Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both servers and gateways. For remote

Table continues…

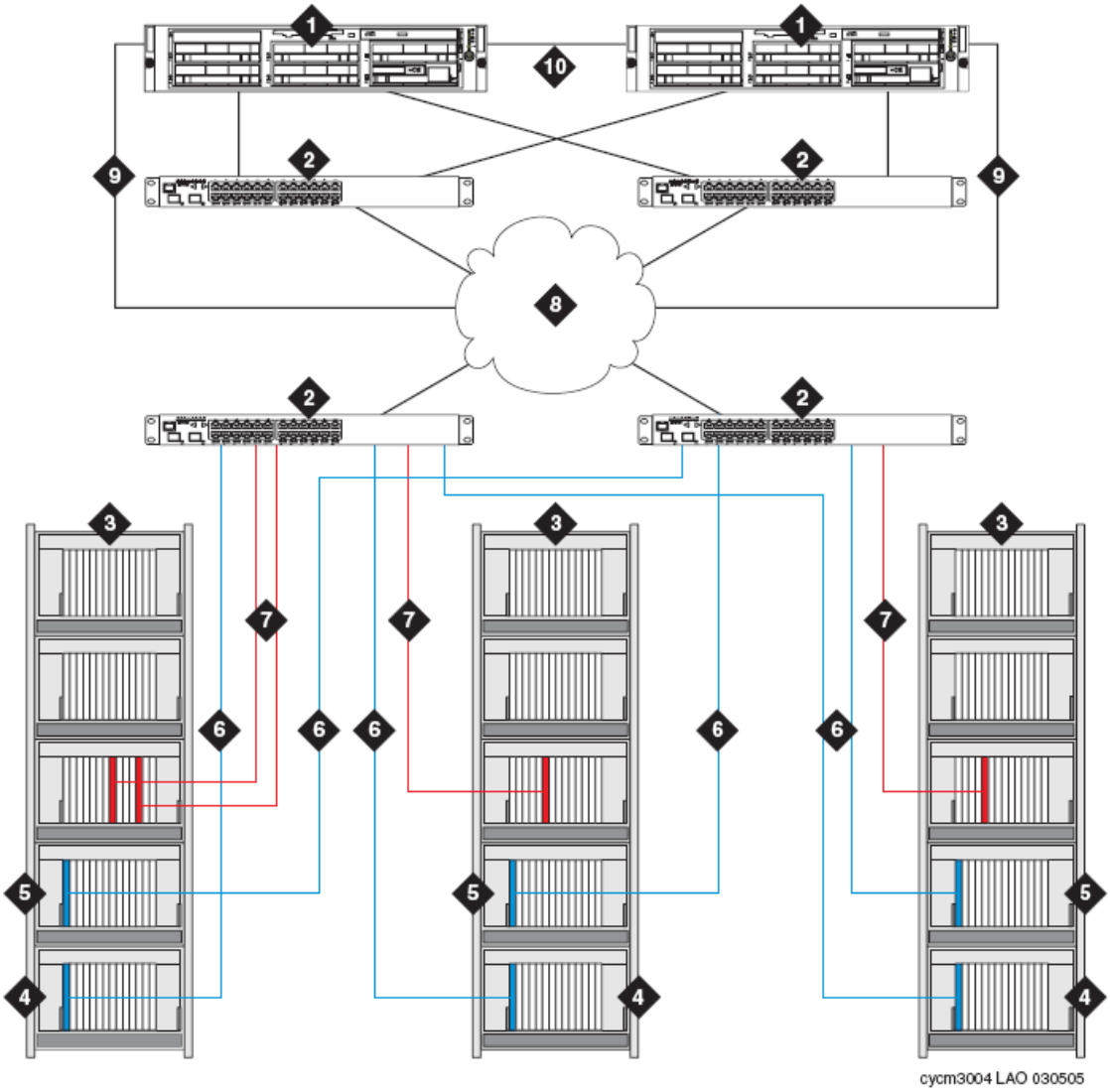
Number	Description
	LAN/WAN connections, the remote gateways must have an Ethernet switch at the remote location.
3	Port networks (G650 Media Gateway or stack).
4	Port network control gateway, in the A position, which contains a TN2312AP/BP IPSI circuit pack for IP connection to server. **Note:** For each physical location of a port network or group of port networks, one port network must also contain a TN771 Maintenance circuit pack. **Note:** For the G650 Media Gateway, the BP version of the TN2312 is required to provide environmental maintenance.
5	IPSI-to-server control network connection via Ethernet switch.
6	LAN connections of TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 for IP-TDM voice processing and optional TN799DP C-LAN for control of IP endpoints. **Note:** The number of TN2302AP, TN2602AP, and TN799DP circuit packs varies, depending on the number of IP endpoints, port networks, and adjunct systems. These circuit packs can be inserted into a port gateway (shown in figure) or the port network control gateway.
7	Customer LAN/WAN.
8	LAN connections of servers for remote administration.
9	Duplicated server links, including the link for translations memory duplication and the link for control data sharing. The link for memory duplication is implemented through the DAL2 adapter or, for the duplex server, through software duplication.

Duplex server IP-PNC for a duplicated control network

The high-reliability configuration of the duplex server IP-PNC is similar to the standard reliability configuration, except for the following differences:

- Duplicated Ethernet switches are available with each server connected to each Ethernet switch.
- Each port network has a duplicated TN2312AP or TN2312BP IPSI circuit pack. You can connect one IPSI circuit pack in each port network through one Ethernet switch and another IPSI circuit pack through another Ethernet switch.

Architecture of duplex IP-PNC duplicated control network



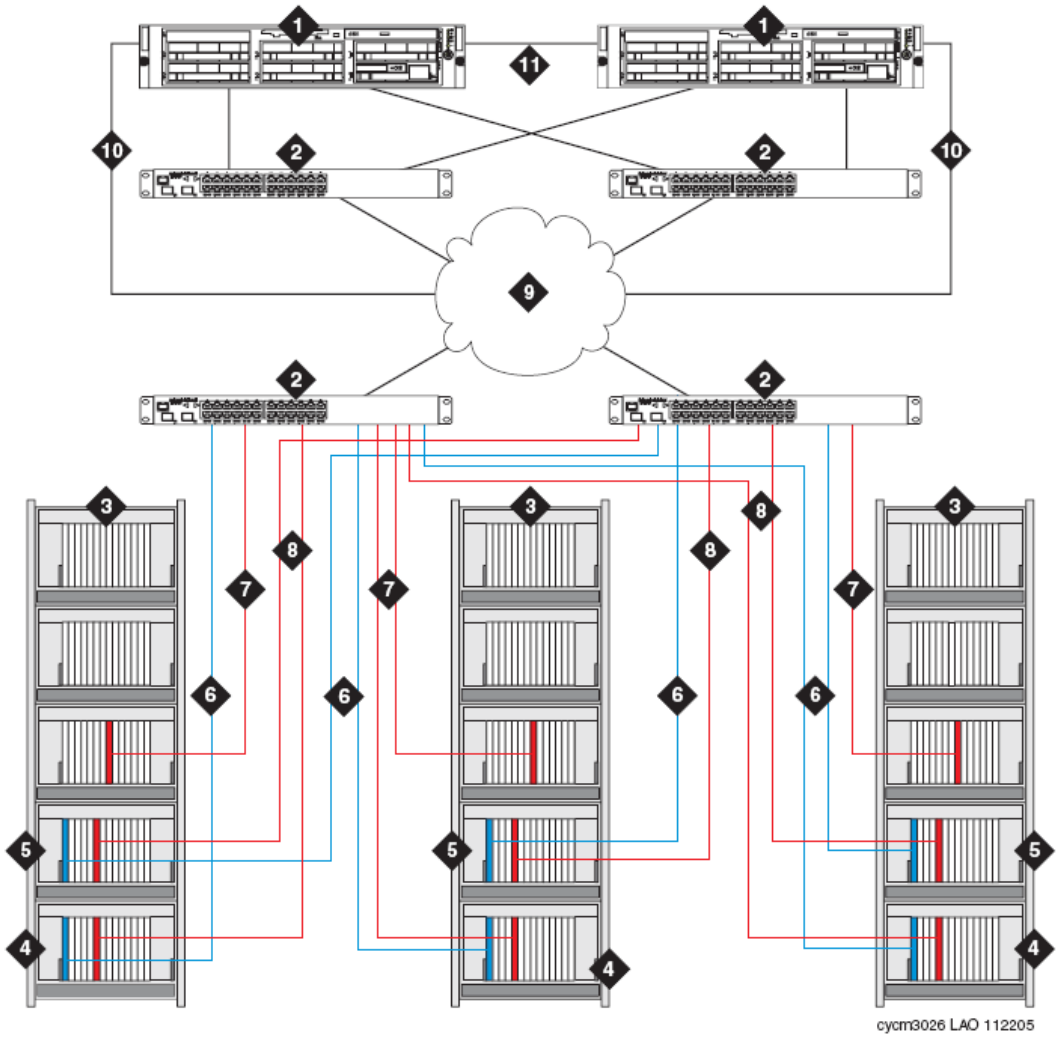
Number	Description
1	Duplex server.
2	Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both the servers and the gateways. For remote LAN/WAN connections, the remote gateways must have an Ethernet switch at the remote location.
3	Port networks (G650 Media Gateway or stack).
4	Port network control gateway, in the A position, which contains a TN2312AP/BP IPSI circuit pack for IP connection to server. **Note:** For the G650 Media Gateway, the BP version of the TN2312 is required to provide environmental maintenance.
5	Duplicated expansion control gateway, in the B position, which contains a TN2312AP/BP IPSI circuit pack for IP connection to control network.
6	IPSI-to-server control network connection via Ethernet switch.
7	LAN connections of TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 for IP-TDM voice processing and optional TN799DP C-LAN for control of IP endpoints. **Note:** The number of TN2302AP, TN2602AP, and TN799DP circuit packs varies, depending on the number of IP endpoints, port networks, and adjunct systems. These circuit packs can be inserted into a port gateway as shown in figure, or the port network control gateway.
8	Customer LAN/WAN.
9	LAN connections of servers for remote administration.
10	Duplicated server links, including the links for translations memory duplication and control data sharing. The link for memory duplication is implemented through the DAL2 adapter or, for the duplex server, through software duplication.

Duplex server IP-PNC for a duplicated control and bearer network connection

The critical-reliability configuration of the duplex server IP-PNC is similar to the high-reliability configuration, except for the following differences:

- Each port network has duplicated TN2602AP IP Media Resource 320 circuit packs. You can connect one TN2602 circuit pack in each port network through one Ethernet switch and another TN2602 circuit pack through another Ethernet switch.
- You must install a TN771DP maintenance test circuit pack in each port network that has duplicated control and bearer network connections.

Architecture of duplex IP-PNC duplicated control and duplicated bearer network



Number	Description
1	Duplex server.
2	Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both the servers and the gateways. For remote LAN/WAN connections, the remote gateways must have an Ethernet switch at the remote location.
3	Port networks (G650 Media Gateway or stack).

Table continues…

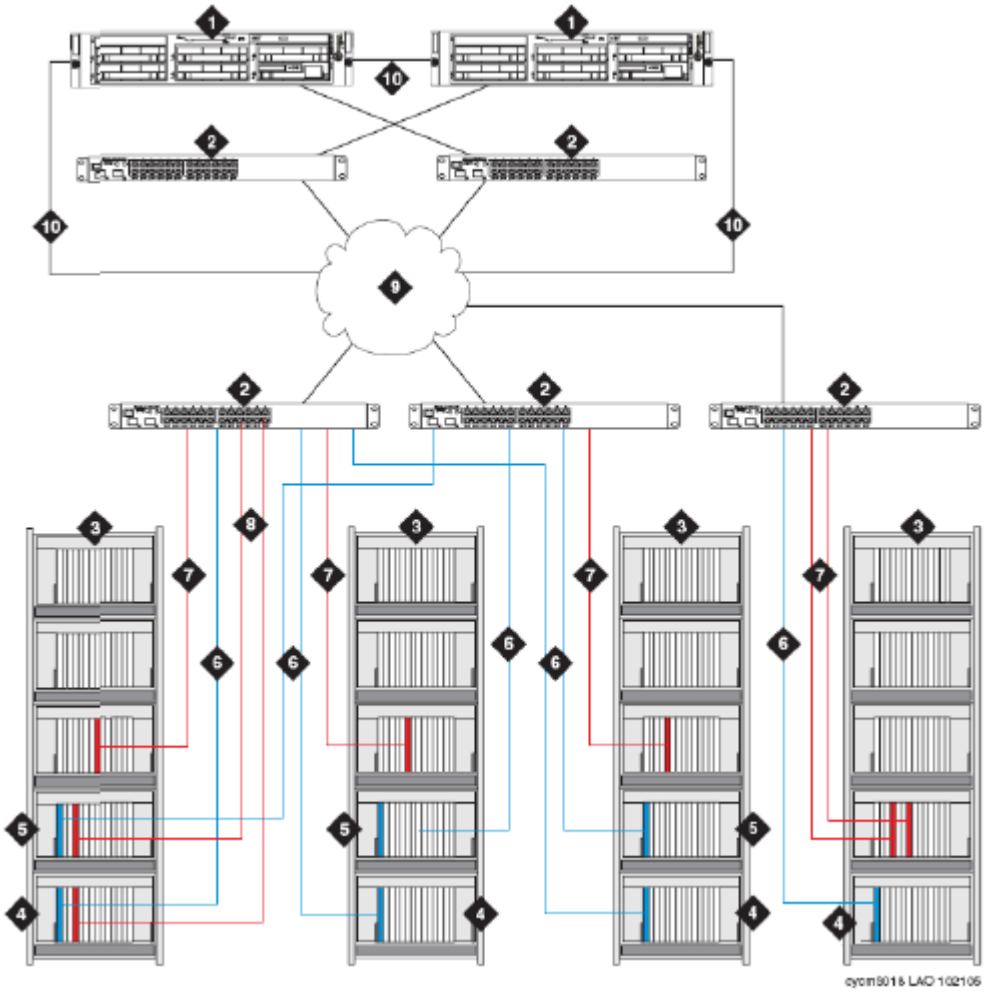
Number	Description
4	Port network control gateway, in the A position, which contains: • A TN2312AP/BP IPSI circuit pack for IP connection to server. **Note:** For the G650 Media Gateway, the BP version of the TN2312 is required to provide environmental maintenance. • A TN2602AP IP Media Resource 320 for port network bearer connections over the LAN **Note:** The TN2602AP circuit pack can be placed in any gateway in the port network. However, separate the pair of TN2602 circuit packs between two different gateways when possible.
5	Duplicated expansion control gateway, in the B position, which contains: • A TN2312AP/BP IPSI circuit pack for IP connection to control network. • A TN2602AP IP Media Resource 320 for port network bearer connections over the LAN **Note:** The TN2602AP circuit pack can be placed in any gateway in the port network. However, the pair of TN2602 circuit packs should be separated between two different gateways whenever possible.
6	IPSI-to-server control network connection via Ethernet switch.
7	LAN connection of the TN799DP C-LAN for control of IP endpoints **Note:** The number of TN799DP circuit packs varies, depending on the number of IP endpoints, port networks, and adjunct systems. These circuit packs can be inserted into a port carrier as shown in figure, the port network control carrier, or the duplicated control carrier.
8	LAN connections of TN2602AP IP Media Resource 320 circuit packs for IP-TDM voice processing.

Table continues…

Number	Description
9	Customer LAN/WAN.
10	LAN connections of servers for remote administration.
11	Duplicated server links, including the link for translations memory duplication and the link for control data sharing. The link for memory duplication is implemented through the DAL2 adapter or, for the duplex server, through software duplication.

Example of IP-PNC port networks with different reliability levels

The following image illustrates a duplex server configuration. This configuration combines duplicated control and duplicated bearer networks, duplicated control-only network, and single control network reliability configurations in an IP-PNC network. The port network with a single control network is labeled as item 11. Other port networks, such as items labeled 3, have duplicated control networks.



Number	Description
1	Duplex server.
2	Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both the servers and the gateways. For remote LAN or WAN connection, the remote gateway must have an Ethernet switch at the remote location.
3	IP-PNC port networks (G650 Media Gateway or stack).
4	Control gateway for port network 3 in the A position in the gateway stack. The control gateway contains a TN2312AP/BP IPSI circuit pack for IP connection to the server.
5	Duplicated port network control gateway for port network 3, in the B position in the gateway stack.

Table continues…

Number	Description
	The control gateway contains a TN2312AP/BP IPSI circuit pack for IP connection to the control network.
6	IPSI-to-server control network connection via Ethernet switch.
7	LAN connections of TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 for IP-TDM voice processing and optional TN799DP C-LAN for controlling IP endpoints. **Note:** The number of TN2302AP, TN2602AP, and TN799DP circuit packs vary, depending on the number of IP endpoints, port networks, and adjunct systems. These circuit packs can be inserted into a port carrier (shown in figure), the port network control carrier, or the duplicated control carrier.
8	Customer LAN or WAN.
9	LAN connections of servers for remote administration.
10	Duplicated server links, including the link for translation memory duplication and the link for control data sharing. The link for memory duplication is implemented through the DAL2 adapter or (for the duplex server) through software duplication.

Chapter 4: 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® Solution Design Considerations and Guidelines*, 03-603978.
- 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.

VoIP hardware

VoIP hardware includes the following components:

- Universal DS1 circuit packs and MM710 T1/E1Media Module on page 43
- TN799DP Control LAN on page 46
- TN2302AP IP Media Processor on page 50
- TN2602AP IP Media Resource 320 on page 51
- TN2312BP IP Server Interface (IPSI) on page 54
- MM760 VoIP Media Module on page 58

Universal DS1 circuit packs and MM710 T1/E1Media Module

The TN464HP/TN2464CP circuit packs and the MM710 Media Module version 3 and later have the same functionality as other DS1 circuit packs. The difference is that the TN464HP/TN2464CP circuit packs and the MM710 Media Module version 3 and later include echo cancellation circuitry and the DS1 does not. The echo cancellation circuitry offers echo cancellation tail lengths of up to 96 milliseconds (ms). The TN574, TN2313, and TN2464 DS1 circuit packs do not support echo cancellation.

The TN464HP/TN2464CP and MM710 are for users who encounter echo over circuits connected to the Direct Distance Dialing (DDD) network. Echo is noticeable when Communication Manager is configured for ATM, IP, and wideband. With these configurations, the delay between the primary signal and the echoed signal is greater than with a TDM configuration. In addition, echo can occur on system interfaces to local service providers that do not routinely install echo cancellation equipment in all the circuits.

Echo cancellation is a right-to-use software feature that supports voice channels and is not intended for data. These circuit packs detect a modem tone and turn off echo cancellation during a data call.

Turn on echo cancellation

About this task

Use this procedure to verify if the echo cancellation is enabled for TN464HP/TN2464CP circuit packs and MM710 T1/E1 Media Modules.

Procedure

1. On the SAT screen, type **`display system-parameters customer-options`**.
2. Ensure that the following fields are complete:
   - **Maximum Number of DS1 Boards with Echo Cancellation**: Specifies the number of DS1 boards that have echo cancellation turned on.
   - **DS1 Echo Cancellation**: Specifies whether echo cancellation is enabled. If the value of this field is `y`, echo cancellation is enabled.

     Note:

     The system can display these fields on different pages of the screen.
3. Exit the screen.

Echo cancellation on the DS1 circuit pack or MM710 media module

For the TN464HP/TN2464CP circuit packs and MM710 media module, use the following fields on the DS1 Circuit Pack screen to support echo cancellation:

- **Echo Cancellation**
- **EC Direction**
- **EC Configuration**

When the Echo Cancellation feature is activated on the System-Parameters Customer Options screen, the system displays the **Echo Cancellation** field. When the **DS1 Echo Cancellation** field is enabled, the system displays the **EC Direction** and **EC Configuration** fields.

EC Direction determines the direction from which echo will be eliminated, either inward or outward. **EC Configuration** is the set of parameters used when cancelling echo.

This information is stored in firmware on the Universal DS1 circuit pack.

Note:

Any changes made to the echo cancellation settings on the DS1 Circuit Pack screen take effect immediately.

Administering the DS1 circuit pack and MM710 media module

Procedure

1. Type `add ds1` *port*, where *port* is the location of the DS1 circuit pack or the MM710 media module.
2. Press `Enter`.

The system displays the DS1 Circuit Pack screen.

3. In the **Echo Cancellation** field, type `y` .

   The system enables echo cancellation on the Universal DS-1 circuit pack.

4. In the **Echo Direction** field, type `inward` or `outward`.

   The system indicates the direction of the echo that is to be cancelled.

5. In the **EC Configuration** field, type digits between 1 to 15. The system indicates the set of parameters used for echo cancellation.

   Note:

   The system displays the **EC Configuration** field on the screen only when the **Echo Cancellation** field is set to `y`.

   For more information about the fields, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

Echo cancellation on trunks

Use the **`change trunk-group`** command to turn echo cancellation on or off for each trunk group. If the **DS1 Echo Cancellation** trunk group field is y, echo cancellation is applied to every TN464HP/ TN2464CP trunk member in that trunk group. The EC Configuration number administered on the DS1 Circuit Pack screen for a trunk board determine the echo cancellation parameters for a trunk member.

Echo cancellation applies to voice channels. The following trunk group types support echo cancellation:

- CO
- TIE
- ISDN-PRI
- FX
- WATS
- DID
- DIOD
- DMI-BOS
- Tandem
- Access
- APLT

Echo cancellation on a trunk group is administered from the TRUNK FEATURES screen.

Note:

Changes to echo cancellation settings on the Trunk Features screen do not take effect until:

- A port or trunk group is busied-out or released.
- The SAT command **`test trunk group`** is run add period.
- Periodic maintenance is performed.

Administering a trunk group for echo cancellation

Procedure

1. Type `change trunk-group`*n,* where *n* is the trunk group number.
2. Go to the Trunk Features page.

   Note:

   Depending on the trunk group type, the system displays different fields on the screen.
3. In the **DS1 Echo Cancellation** field, type `y` to enable echo cancellation for each trunk group.
4. Save the changes.

TN799DP Control LAN

Systems in a private network are interconnected by both tie trunks for voice communications and data links for control and transparent feature information. Various DS1, IP, and analog trunk circuit packs provide the voice communications interface. For TCP/IP connectivity, the data-link interface is provided by a TN799DP Control LAN (C-LAN) circuit pack. For more information about this VoIP transmission hardware, see VoIP transmission hardware on page 18 .

C-LAN handles the data-link signaling information in the Ethernet or point-to-point (PPP) configuration. The C-LAN circuit pack has one 10/100BaseT Ethernet connection and up to 16 DS0 physical interfaces for PPP connections. C-LAN also extends ISDN capabilities to csi models by providing packet-bus access.

- In the Ethernet configuration, C-LAN passes the signaling information over a separate TCP/IP network, usually by a hub or Ethernet switch.

  Use an Ethernet switch for optimal performance. For this configuration, install the C-LAN circuit pack and connect the appropriate pins of the C-LAN I/O field to the hub or Ethernet switch.
- In the PPP configuration, C-LAN passes the data-link signaling to the DS1. The data-link signaling is then included in the same DS1 bit stream as the DCS voice transmissions.

  For this configuration, install the C-LAN circuit pack No other connections are needed. You must install the appropriate DS1 circuit packs if the circuit packs are not already present.

Physical addressing for the C-LAN board

The Address Resolution Protocol (ARP) on the C-LAN circuit pack relates the 32-bit IP address configured in software to the 48-bit C-LAN circuit pack MAC address. The MAC address is burned into the board at the factory. The C-LAN board has an ARP table that contains the IP addresses associated with each hardware address. This table is used to route messages across the network. Each C-LAN board has one MAC address, one Ethernet address, and up to 16 PPP addresses.

IP addressing techniques for the C-LAN board

C-LAN supports both Classless Inter-domain Routing and Variable-Length Subnet Masks. These addressing techniques provide greater flexibility in addressing and routing than class addressing alone.

Installing the TN799DP C-LAN

Before you begin

TCP/IP connections, Ethernet, or PPP require a TN799DP C-LAN circuit pack, unless your system has embedded Ethernet capabilities. Before you install the C-LAN circuit pack, ensure you understand the requirements of your LAN. For information about LAN requirements for VoIP, go to http://www.extremenetworks.com/LIBRARIES/Avaya/AvayaIPvoiceQualityNetworkRequirements.pdf and read the white paper titled *Avaya IP Voice Quality Network Requirements (EF-LB1500)*.

About this task

Use this procedure to install the TN799DP C-LAN.

Note:

You do not need to switch off the cabinet to install a C-LAN circuit pack.

Procedure

1. Determine the carrier or slot assignments of the circuit packs to be added.

   You can insert the C-LAN circuit pack into any port slot.

2. Insert the circuit packs into the slots you determined in Step 1.

   Note:

   You do not need to switch off the cabinet to install a C-LAN circuit pack.

Connecting C-LAN cables to a hub or Ethernet switch

Before you begin

In the Ethernet configuration, the C-LAN passes the signaling information over a separate TCP/IP network, usually by a hub or Ethernet switch. Connect the appropriate pins of the C-LAN I/O field to the hub or Ethernet switch.

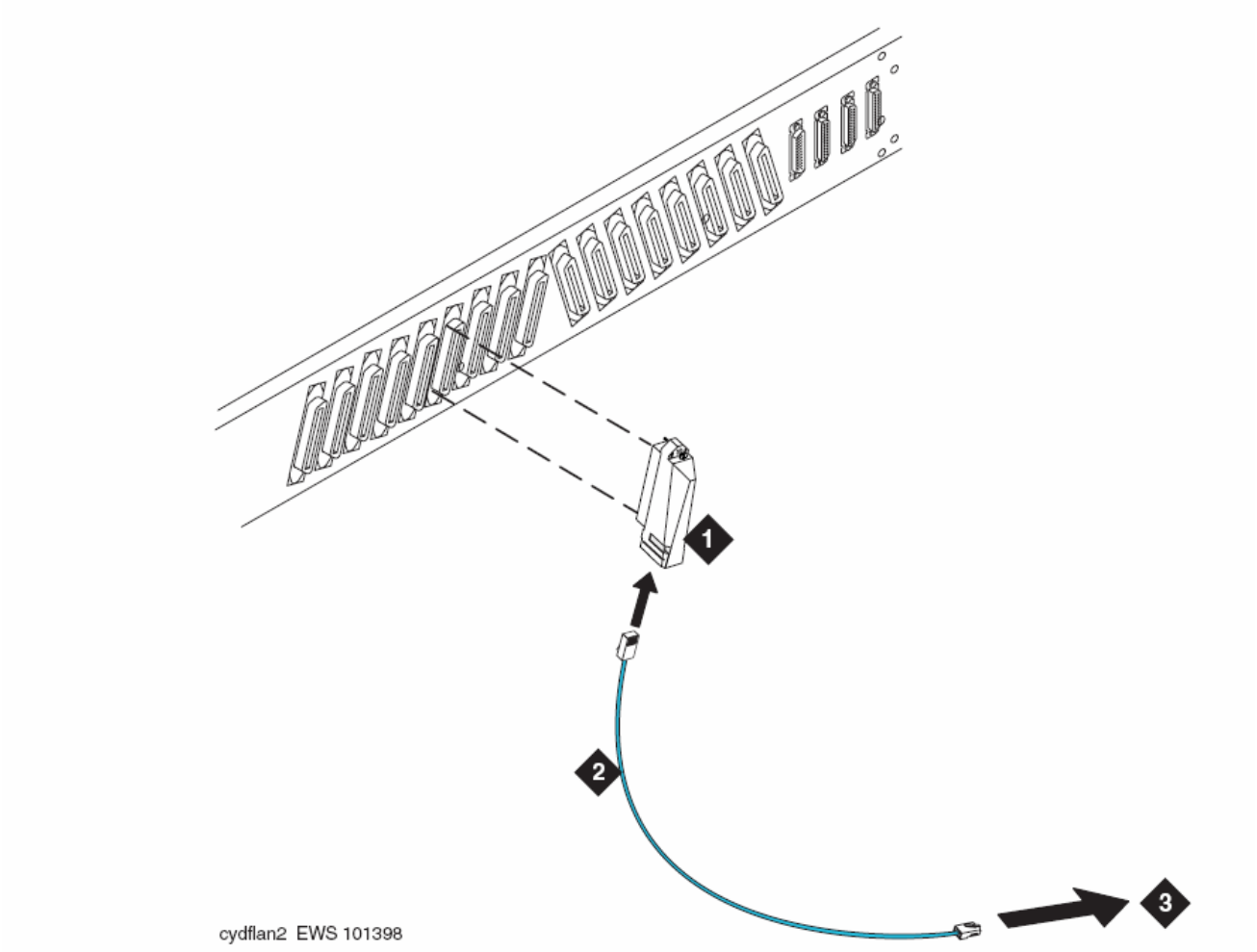
Procedure

1. Connect the 259A connector to the backplane of the port slot containing the C-LAN circuit pack.

2. Connect the Category 5 UTP cable to the 259A connector and a hub or Ethernet switch.

   Port 17 on the C-LAN circuit pack is now connected to the LAN.

Cable connection for C-LAN connectivity



Name	Description
1	259A Connector
2	Category 5 UTP Cable with a maximum length of 100 m
3	Ethernet switch

LAN default gateway

On LANs that connect to other networks or subnetworks, define a default gateway. The default gateway node is a routing device that is connected to different networks or subnetworks. Any packets addressed to a different subnetwork, and for which no explicit IP route is defined, are sent to the default gateway node.

You must use the IP Interfaces screen to administer a node such as C-LAN port, PROCR, or IP Interface port, as the default gateway.

The default node on the Node Names screen is a display-only entry with IP address 0.0.0.0. The IP address 0.0.0.0 functions as a variable that takes on unknown addresses as values. While setting up the default IP route, any address that the C-LAN cannot process is substituted for the default address in the default IP route.

Alternate Gatekeeper and C-LAN load balancing

Alternate Gatekeeper gives IP endpoints a list of available C-LAN circuit packs. Alternate Gatekeeper addresses and C-LAN load-balancing spread IP endpoint registration across more than one C-LAN circuit pack. The C-LAN load-balancing algorithm allocates endpoint registrations within a network region to the C-LAN with the least number of sockets in use. Using this C-LAN load-balancing algorithm increases system performance and reliability.

The software registers with the original C-LAN circuit pack IP address. Then the software sends back the IP addresses of all C-LAN circuit packs in the network region of the IP endpoint. If the network connection to one C-LAN circuit pack fails, the IP endpoint reregisters with a different C-LAN. If the system uses network regions based on the IP address, the software also sends the IP addresses of C-LANs in interconnected regions. These alternate C-LAN addresses are also called gatekeeper addresses. These addresses can be used when the data network carrying the call signaling from the original C-LAN circuit pack fails.

IP telephones can be programmed to search for a gatekeeper independently of load balancing. The IP telephone accepts gatekeeper addresses in the message from the Dynamic Host Configuration Protocol (DHCP) server. It also accepts addresses in the script downloaded from the Trivial File Transfer Protocol (TFTP) server. too long If the telephone cannot contact the first gatekeeper address, the telephone uses an alternate address. If the first gatekeeper rejects the extension and password , the IP phone contacts the next gatekeeper. The number of gatekeeper addresses that the telephone accepts depends on the length of the addresses administered on the DHCP server.

Note:

A single Alternate Gatekeeper list is usually used in configurations with multiple servers. In this case, the DHCP server sends the same Alternate Gatekeeper list to all IP endpoints. However, if an IP endpoint is unable to register with some of the gatekeepers in the list, a registration attempt to those gatekeepers is rejected.

C-LAN load balancing and alternate gatekeeper addresses require IP stations that accept multiple IP addresses, such as:

- IP telephone
- IP softphone
- Avaya IP Agent

Endpoint capabilities

Table 1: Endpoint capabilities

Endpoint	Number of Gatekeepers	Settings
IP Telephone	1 8 10 72	Default DNS name AvayaCallServer, or manually, one fixed IP address. Through DHCP-DNS names or fixed IP addresses. DHCP limits all options to 255 bytes. Through TFTP-DNS names or fixed IP addresses. TFTP overwrites any gatekeepers provided by DHCP. Fixed IP addresses from Communication Manager. Communication Manager 2.0 and later supersede any gatekeeper address provided earlier.
IP Softphone R5	30	Manually through options or properties of the IP Softphone after the IP Softphone is installed.
IP Agent R3	30	Manually through options or properties of the IP agent after installation, or from Communication Manager.

Note:

DHCP servers send a list of alternate gatekeeper and C-LAN addresses to the IP Telephone endpoint. A hacker can send a false request and thereby get IP addresses from the DHCP server. However, the alternate gatekeeper IP addresses are sent only to an endpoint that successfully registers.

TN2302AP IP Media Processor

Use the TN2302AP IP Media Processor to send voice and FAX data with non-DCS signaling over IP connections. This Media Processor also transmits voice and Fax data for H.323 multimedia applications in H.323 V2 compliant endpoints.

The TN2302AP IP Media Processor provides port network connectivity for an IP-connected configuration. The TN2302AP IP Media Processor includes a 10/100BaseT Ethernet interface to support H.323 endpoints for IP trunks and H.323 endpoints. The TN2302AP IP Media Processor design improves voice quality through dynamic jitter buffers.

The TN2302AP IP Media Processor also performs the following functions:

- Echo cancellation
- Silence suppression
- DTMF detection
- Conferencing

The TN2302AP IP Media Processor supports the following codecs:

- G.711 (mu-law or a-law, 64 Kbps)
- G.723.1 (6.3 Kbps or 5.3 Kbps audio)
- G.729 (8 Kbps audio)

The TN2302AP IP Media Processor also supports FAX detection and conversion between these codecs. remove space before the period

TN2302AP transmission interface

The TN2302AP IP Media Processor uses dynamic jitter buffers to provide improved voice quality. The digital signal processors (DSPs) of the TN2302AP insert the following loss or gain by default:

- 5.0 dB of loss in the signal from the IP endpoints
- 5.0 dB of gain in the signal to the IP endpoints

Based on the country code on the terminal-parameters screen, system administrators can administer the loss or gain.

TN2302AP hairpinning

The TN2302AP IP Media Processor supports 64 ports of shallow hairpin. IP packets that do not require speech codec transcoding can be looped back at the UDP/IP layers with a change of address. By looping back , you can reduce delay and make DSP resources available.

TN2302AP ports

The TN2302AP IP Media Processor is a service circuit pack, not a trunk circuit pack. Therefore, an H.323 tie trunk cannot be used for facility test calls. Use the **`ping`** command to test the TN2302AP ports.

TN2602AP IP Media Resource 320

For local stations and outside trunks, the TN2602AP IP Media Resource 320 provides high-capacity voice over Internet protocol (VoIP) audio access to the switch . The IP Media Resource 320 provides audio processing for the following types of calls:

- TDM-to-IP and IP-to-TDM
- IP-to-IP

The TN2602AP IP Media Resource 320 circuit pack has two capacity options, both of which are determined by the license file installed on Communication Manager:

- 320 voice channels, considered the standard IP Media Resource 320
- 80 voice channels, considered the low-density IP Media Resource 320

The port network can hold only two TN2602AP circuit packs.

Note:

CMC1 and G600 branch gateways do not support the TN2602AP IP Media Resource 320.

Load balancing

For load balancing, up to two TN2602AP circuit packs can be installed in a single port network. The TN2602AP circuit pack is also compatible with and can share load balancing with the TN2302 and TN802B IP Media Processor circuit packs. The actual capacity can be affected by a variety of factors, including the codec used for a call and fax support.

Note:

When you use two TN2602AP circuit packs, each with 320 voice channels, for load balancing within a port network, you get 484 voice channels. This limit for the number of voice channels depends on the maximum number of time slots available for a port network, that is 484.

Bearer duplication

You can install two TN2602AP circuit packs in a single port network to achieve duplication of the bearer network. In this configuration, one TN2602AP is an active IP media processor and the other one is a standby IP media processor. If the active media processor or connections to the media processor fail, active connections failover to the standby media processor and remain active. This duplication prevents active calls in progress from being dropped during failure. The interchange between duplicated circuit packs affects only the port network in which the circuit packs reside.

Note:

The 4606, 4612, and 4624 IP telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from the active to the standby media processor is in process, then calls might be dropped.

Virtual IP and MAC addresses to enable bearer duplication

Duplicated TN2602AP circuit packs in a port network share a virtual IP address and a virtual MAC address. The currently active TN2602 owns these virtual addresses. Each TN2602 also has a real IP address. All bearer packets sent to a port network that contains duplicated TN2602AP circuit packs are sent to the virtual IP address of the TN2602 pair in that port network. The bearer packets are sent regardless of whether the packets originate from TN2602s in other port networks or from IP telephones or gateways. The active TN2602AP circuit pack receives those packets.

During failover to the standby TN2602, the TN2602s negotiate with each other to determine which TN2602 is active and which is standby. State-of-health, call state, and encryption information is shared between TN2602s during this negotiation. The newly active TN2602AP circuit pack sends a gratuitous address resolution protocol (ARP) request. With this ARP request, the circuit pack ensures that the LAN infrastructure is updated appropriately with the location of the active TN2602. Other devices within the LAN update the old mapping in ARP cache with the new mapping.

Requirements for bearer duplication

The Communication Manager license file must have entries for each circuit pack. The entries must have identical voice channels enabled. In addition, both circuit packs must have the latest firmware that supports bearer duplication.

Duplicated TN2602AP circuit packs must be in the same subnet. The Ethernet switch or switches that the circuit packs connect to must also be in the same subnet. Ethernet switches can use signals from the TN2602AP firmware to identify the MAC address of the active circuit pack when switches share subnets. This identification process provides a consistent virtual interface for calls.

Duplication and load balancing

A single port network can have only up to two TN2602AP circuit packs. Therefore, the port network can only have either two duplicated TN2602AP circuit packs or two load balancing TN2602AP circuit packs. However, in a Communication Manager configuration, some port networks can have a duplicated pair of TN2602AP circuit packs and other port networks can have a load balancing pair of TN2602AP circuit packs. Some port networks can also have a single TN2602AP circuit pack or none.

Note:

A pair of TN2602AP circuit packs previously used for load balancing can be readministered to be used for bearer duplication. After readministration, only the voice channels of the active circuit pack can be used. For example, in two TN2602 AP circuit packs in a load balancing configuration with 80 voice channels in each, iff you readminister the circuit packs to be in the bearer duplication mode, only 80 channels are available. Similarly, in two TN2602 AP circuit packs in a load balancing configuration with 320 voice channels in each, if you readminister the circuit packs to be in bearer duplication mode, only 320 channels are available.

TN2602AP IP Media Resource 320 features

The IP Media Resource 320 supports hairpin connections and the shuffling of calls between TDM connections and IP-to-IP direct connections. The IP Media Resource 320 can also perform the following functions:

- Echo cancellation
- Silence suppression
- Adaptive jitter buffer of up to 320 milliseconds
- Dual-tone multifrequency (DTMF) detection
- AEA Version 2 and AES media encryption
- Conferencing
- QOS tagging mechanisms in layer 2 and 3 switching (Diff Serv Code Point [DSCP] and 802.1pQ layer 2 QoS)
- RSVP protocol

The TN2602AP IP Media Resource 320 circuit pack supports the following codecs for voice, conversion between codecs, and fax detection:

- G.711, A-law or Mu-law, 64 kbps
- G.726A 32 kbps
- G.729 A/AB, 8 kbps audio

The TN2602AP also supports transport of the following devices:

- Fax, Teletypewriter device (TTY), and modem calls using the pass-through mode
- Fax, V.32 modem, and TTY calls using the proprietary relay mode

  Note:

  V.32 modem relay is needed primarily for secure SCIP telephones, formerly known as Future Narrowband Digital Terminal (FNBDT) telephones, and STE BRI telephones.
- T.38 fax over the Internet, including endpoints connected to non-Avaya systems
- 64-kbps clear channel transport in support of firmware downloads, BRI secure telephones, and data appliances

Firmware download

The IP Media Resource 320 can serve as an FTP or SFTP server for firmware downloads. However, only authorized services personnel can activate and use this capability.

As with the TN2302AP IP Media Processor, firmware upgrades of the TN2602AP circuit pack are not call maintaining. However, by using the **`campon-busyout media-processor`** command, a single or load balanced TN2602AP circuit pack can be busied out without dropping calls, and then upgraded. In addition, with duplicated TN2602AP circuit packs, the standby TN2602AP circuit pack can be upgraded first, and then the circuit packs can be interchanged. The active circuit pack becomes the standby and can then be busied out and upgraded without dropping calls.

I/O adapter

The TN2602AP IP Media Resource 320 circuit pack has a services Ethernet port in the faceplate. The TN2602AP circuit pack requires an input/output adapter that provides for one RS-232 serial port and two 10/100 Mbps Ethernet ports for LAN connections. However, only the first Ethernet port is used. This Ethernet connection is made at the back of the IP Media Resource 320 slot.

Note:

The TN2302AP IP Media Processor can also use this I/O adapter.

TN2312BP IP Server Interface

In configurations with the duplex server controlling gateways, the bearer paths and the control paths are separate. Control information for port networks travel over a LAN through the Ethernet switch. The control information ends on the duplex server at one end and on a TN2312BP IP Server

Interface (IPSI) on the other end. Each IPSI can control up to five port networks by tunneling control messages over the Center-Stage or ATM network to port networks without IPSIs.

Note:

You cannot put IPSIs in a port network that has a Stratum-3 clock interface. Also, you cannot put IPSIs in a remote port network that is using a DS1 converter.

In configurations that use a dedicated LAN for the control path, IPSI IP addresses are usually assigned automatically using DHCP service from the server. Also, a dedicated IPSI Ethernet connection to a laptop can be used to assign static IP addresses or for maintenance. In configurations using the customers LAN, only static addressing is supported.

For information about installing and upgrading duplex servers and IPSI configurations, see the *Avaya S8300, Simplex and Duplex server Library* CD, 555-233-825.

You can use the **`status qos-parameters ipserver-interface`** command to view the ISPI settings. The board location must be a valid TN2312 or TN8412 board location. For more information about the **`status qos-parameters ipserver-interface`** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431.

Detailed description

In Communication Manager Release 5.2, an administrator can manage the following IPSI-related parameters using a SAT interface or System Management Interface:

- On the System Parameters IP Server Interface screen, set the values of the **DiffServ** and **802.1p** QoS parameter fields . The default value for **DiffServ** is 46 and the value for **802.1p** is 6.
- Download QoS parameters to all IPSI boards. By default, the **`add ipserver-interface`** or **`change ipserver-interface`** command prepopulates the QoS parameters when IPSI boards are added.
- On the IP Server Interface screen, set the values of **Auto**, **Speed**, or **Duplex** Ethernet interface fields . **Speed** and **Duplex** fields display on the IPSI screen if the **Auto** field is set to n.
- On the IP Server Interface screen, change IPSI IP addresses in the **IP Address**, **Subnet Mask**, and **Gateway address** fields .

  Note:

  Set the initial IPSI IP address manually by locally logging on to each IPSI board through a telnet or an ssh connection. This topic has actions; rewrite as a task topic with a suitable heading.

Firmware

The IPSI and Communication Manager use a capabilities exchange message to determine whether an IPSI/SIPI board can support the IPSI administration feature. To support the capabilities exchange message after the port network is in service, you require:

- IPSI firmware version 46 or later

- SIPI firmware version 16 or later

IP Server Interface parameters

The IPSI sends QoS parameters, Ethernet settings, and IP address information to Communication Manager as specified in the *IP Server Interface parameters* table. The exchange of information is shared on socket creation.

Warning:

The Ethernet interface settings Auto, Speed, and Duplex, or the IPSI IP address settings IP Address, Subnet Mask, and Gateway address must match with the network entity that the IPSI is communicating with. In case these parameters do not match, network communication can stop. To recover the settings, you must go to the physical site of the IPSI, log in to the IPSI services port, and change the settings.

Table 2: IP Server Interface parameters

Description	Conditions/Comments	Required board is busied out
QoS parameters: On the System Management Interface, select **Installation** > **Configure Server**. and enable VLAN 802.1q priority tagging. On the IP Server Interface screen, you can use System Level Parameter Values and update the following parameters: **802.1p** **DiffServ**		No
Ethernet interface settings: On the IP Server Interface screen, update values for the following parameters: Auto Speed Duplex	Reset the IPSI board for **Auto**, **Speed**, and **Duplex** values to take effect.	Yes
IP Address information: On the IP Server Interface screen, update values for the following parameters: IPSI **IP Address** Subnet Mask **Gateway** address	Reset the IPSI board for **IP Address**, **Subnet Mask**, and **Gateway** address values to take effect.	Yes

Communication Manager alarm on settings mismatch

Communication Manager compares the values administered on SAT with the reported IPSI board values. The system generates a warning alarm if Communication Manager finds any discrepancies in the following values:

- **802.1p**
- **DiffServ**
- Ethernet **Auto**
- Ethernet **Speed**
- Ethernet **Duplex**

You can view the alarm using the **`display alarms`** command or by entering error type `1` on the Display Errors screen.

Note:

Discrepancy between the SAT administration and the IPSI board values can happen if you change any IPSI board values using the CLI.

You can clear the alarm in one of the following ways:

- Set the correct values, and busyout or release the IPSI board.
- Change the values on the IP Server Interface screen, and submit the screen.
- Change the values on the affected IPSI board using the CLI .

Default settings of IPSI QoS parameters

In the IPSI administration feature, QoS settings are standardized to communicate between the IPSI and Communication Manager. If required, you can administer the QoS parameters on the Change IP Server Interface screen. The QoS default settings are shown in the following table:

Table 3: QoS default settings

Description	Default settings	Location
Communication Manager to IPSI	**DiffServ** = 46	**DiffServ** field on **`change ipserver-interface`** SAT screen.
	802.1p = 6	**802.1p** field on **`change ipserver-interface`** SAT screen.
	802.1p/Q enabled = no	On the System Management Interface, select **Installation** > **Configure Server**. The system displays the Configure Server wizard. Click **Configure Interface**.
IPSI to Communication Manager	**DiffServ** = 46 (vintage >= 38) **DiffServ** = 40 (vintage < 38)	**DiffServ** field on **`change ipserver-interface`** SAT screen. Or IPSI CLI interface.

Table continues…

Description	Default settings	Location
	802.1p = 6	**802.1p** field on **`change ipserver-interface`** SAT screen. Or IPSI CLI interface.
	802.1p/Q enable = no	IPSI CLI interface.

Backward compatibility

The IPSI administration interoperates with Communication Manager Release 5.0 or earlier by using the preexisting QoS and administration interface. An IPSI uses the IPSI administration feature if IPSI firmware version is 46 or later, SIPI firmware version is 16 or later, and the Communication Manager system supports Release 5.2 features.

The IPSI administration feature with Communication Manager Release 5.2 works with earlier IPSI boards as follows:

- Communication Manager assesses the administration capability of an IPSI board based on the capabilities exchange message.
- In general, if an older IPSI cannot support this feature, then you must administer that IPSI by using the CLI . If Communication Manager cannot exchange the capabilities message with an older IPSI board, the following happens:
  - Communication Manager stops sending any IPSI QoS or Ethernet settings to IPSI.
  - Communication Manager stops receiving the IPSI QoS or Ethernet settings from IPSI.
  - IPSI reports the IPSI status on the IP Server Interface screen.

MM760 VoIP Media Module

The Avaya MM760 Media Module is a clone of the motherboard VoIP engine. MM760 provides the audio bearer channels for VoIP calls and is controlled by the G700. Based on system administration of audio codecs, MM760 can handle either 64 or 32 simultaneous channels of H.323 audio processing. If the IP Parameters screen specifies only G.711 mu-law or G.711 a-law as the audio codecs, MM760 can service 64 channels. If any other codec type, such as G.723-5.3K, G.723-6.3K, or G.729, is administered, MM760 can only service 32 channels. These call types can be mixed on the same resource. In other words, the simultaneous call capacity of the resource is 64 G.711 Equivalent Calls.

Note:

Customers who want an essentially nonblocking system must add an additional MM760 Media Module. An additional MM760 Media Module is required only if customers use more than two MM710 Media Modules in a single chassis. The extra MM760 provides an additional 64 channels and is supported by only G700 Branch Gateway. MM760 is not supported by G250, G350, G430, and G450 branch gateways.

MM760 Ethernet interface

MM760 must have an Ethernet address. The MM760 requires a 10/100Base T Ethernet interface to support H.323 endpoints for Avaya IP trunks and stations from another G700 Branch Gateway. The G700 Branch Gateway supports MM760, but G250, G350, G430, and G450 branch gateways do not.

Voice compression on MM760

MM760 supports on-board resources for compression and decompression of voice. The compression and decompression is for A and μ-law G.711, G.729, G.729B, and 5.3K and 6.3K G. 723. The VoIP engine supports the following functionality:

- RTP and RTCP interfaces
- Dynamic jitter buffers
- DTMF detection
- Hybrid echo cancellation
- Silence suppression
- Comfort noise generation
- Packet loss concealment

MM760 also supports transport of the following:

- Teletypewriter device (TTY) tone relay over the Internet
- Faxes over a corporate IP intranet: Only on Avaya telecommunications and networking equipment.

  Security alert:

  Faxes sent to non-Avaya endpoints cannot be encrypted.
- Modem tones over a corporate IP intranet: Only on Avaya telecommunications and networking equipment.

Avaya gateways

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

- *Administering Avaya Aura® Communication Manager*, 03-300509
- *Upgrading, Migrating, and Converting Servers and Branch Gateways*, 03-300412

Avaya Aura® Media Server

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

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 4: 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

Table continues…

Number length	NPI=Public	NPI=Private	NPI=Unknown
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.

The TN2302AP or TN2602AP enables H.323 trunk service using IP connectivity between an Avaya IP solution and another H.323 v2-compliant endpoint.

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.

Administering C-LAN and IP Media Processor circuit packs for simplex/duplex servers

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 to administer as a 4602
- 4602SW to administer as a 4602
- 4690 to 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 the system successfully registers the phone, 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 dual-connection architecture IP Telephones R2 or earlier, 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.

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 116.

Related links

Setting network performance thresholds on page 111

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
- C-LAN Ethernet or PPP IP Address
- Bridge or router IP Address

- CMS IP Address
- Communication Manager Messaging Address

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

For H.323 connections, each MedPro Ethernet port (IP interface) 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.

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 C-LAN Ethernet port on the network
   - Each IP Media Processor
   - 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.

Defining IP interfaces for duplicated TN2602AP

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 changed. 802.1p/Q settings in Communication Manager must match the settings in all interfacing elements in your data network.

Related links

IP Network Region field descriptions on page 130

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 Codec Set screen. location must precede action.

2. Assign each codec set to the appropriate network region.
3. Assign the network region to the appropriate devices:
   - TN2302AP or TN2602AP
   - Avaya G250, G350, G430, G450, or G700 Branch Gateway

   .
4. If the TN2302AP or TN2602AP 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 102
Defining IP interfaces on page 66
IP codec sets on page 125
IP network regions on page 128
Manually interconnecting the network regions on page 139

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*, 03-300509.

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 C-LAN 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 C-LAN 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 (C-LAN). 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 C-LAN 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*, 03-602878.

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*, 03-300509.

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.

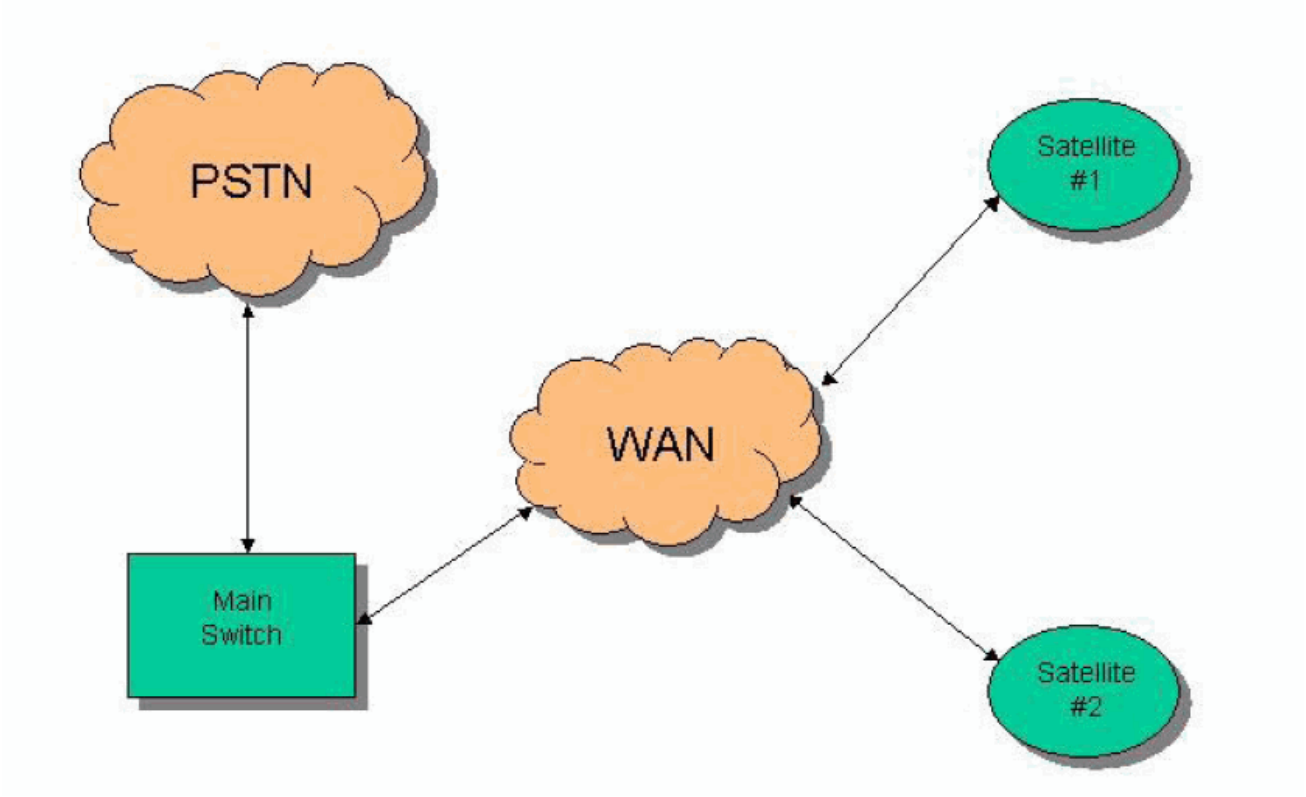


Figure 5: Private/public calling party numbers (CPN)

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 74
- Avaya IP telephones on page 77

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 nonsoftphone 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*, 03-300509.

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*, 03-300509.

The two main types of IP Softphone configurations are:

- Administering a Telecommuter Telephone on page 75
- Administering a Road-warrior telephone on page 76

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

     This field specifies the maximum number of remote office 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*, 555-245-207, or the appropriate IP Telephone user guides.

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

- *4600 Series IP Telephone Installation Guide, 555-233-128*
- *4600 Series IP Telephone LAN Administrator's Guide, 555-233-507*

- *Avaya one-X Deskphone Edition 9600 Series IP Telephone Installation and Maintenance Guide, 16-300694*
- *Avaya one-X Deskphone Edition 9600 Series IP Telephones Administrator Guide, 16-300698*
- *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide, 16-601438*
- *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Administrator Guide Release 1.0, 16-601443*

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

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.

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. For more information on managing the firmware and configuration files for the 4600-series IP telephones during Communication Manager upgrades, see *Installing and Upgrading the Avaya G700 Branch Gateway and Avaya S8300D*, (555-234-100), or *Upgrading, Migrating, and Converting Servers and Gateways*, (03-300412).

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 TN2302AP IP Media Processor or TN2602AP Media Resource 320 circuit pack. 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.

The 4600-series IP telephone also requires a TN799DP Control-LAN (C-LAN) circuit pack for the signaling capability on the DEFINITY Server csi platform. You do not need a C-LAN circuit pack to connect an IP telephone if your system has built-in capability, for example, using an Avaya S8300D server, Avaya S8300E server or Avaya Duplex server. You also do not require a C-LAN circuit pack if the system has Processor Ethernet capability.

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

Installing TN2302AP, TN2602AP, and TN799DP circuit packs

Procedure

1. Determine the carrier or slot assignments of the circuit packs to be added.
2. Insert the circuit pack into the appropriate slot.

Note:

You do not have to switch off the cabinet to install the circuit packs.

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 TN2302AP IP Media Processor and TN2602AP IP Media Resource 320.
- Bypass the TDM bus, conserving timeslots.
- Improve voice quality by bypassing the codec on the TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit packs.

Shuffling releases more resources on the TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit packs 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 TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 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 TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack 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 TN2302AP or TN2602AP channels and TDM bus time slots and improves voice quality by bypassing codec of the TN2302AP or TN2602AP. Both endpoints must be capable of shuffling, that is, support H.245 protocol before Communication Manager can shuffle a call.

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 95 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 TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit packs.

Examples of shuffling

Shuffling within the same network region

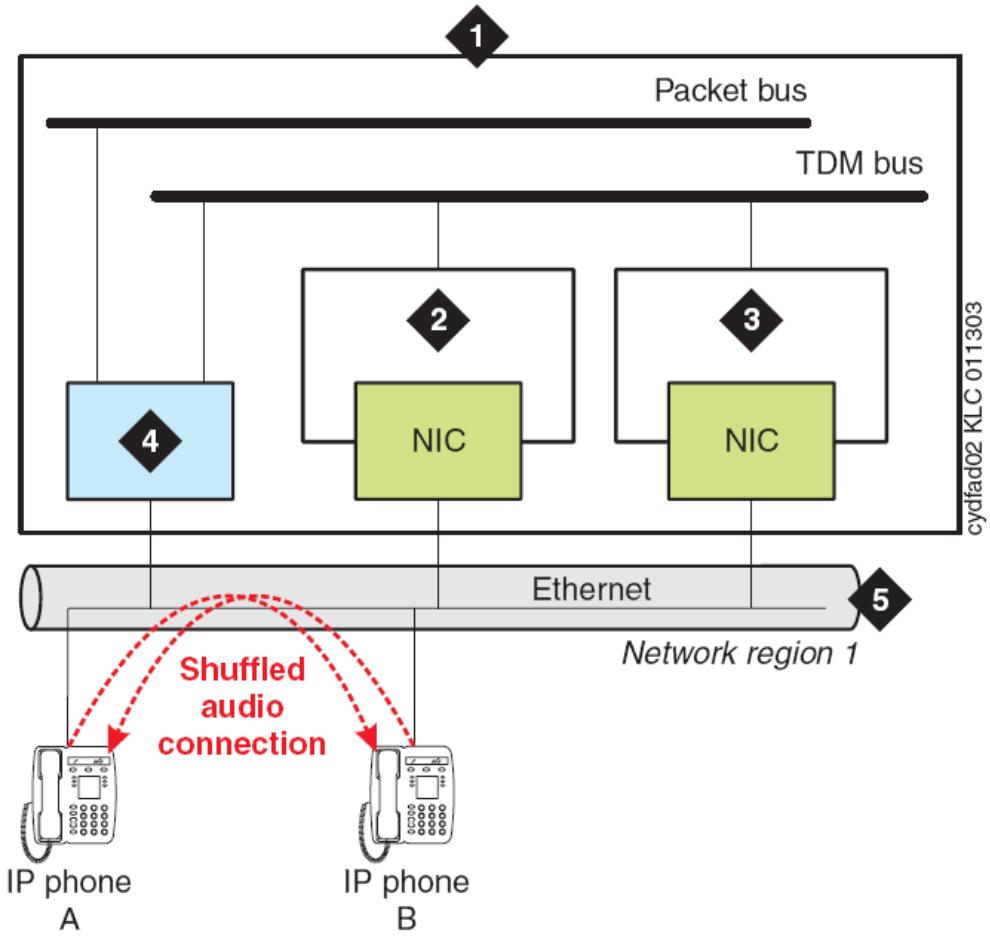


Figure 6: Shuffled audio connection between IP endpoints in the same network region

Number	Description
1	Avaya server
2	TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit pack
3	TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit pack
4	TN799 Control LAN (C-LAN) circuit pack
5	LAN/WAN segment administered in Communication Manager as network region 1

Shuffling within the same network region on page 83 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

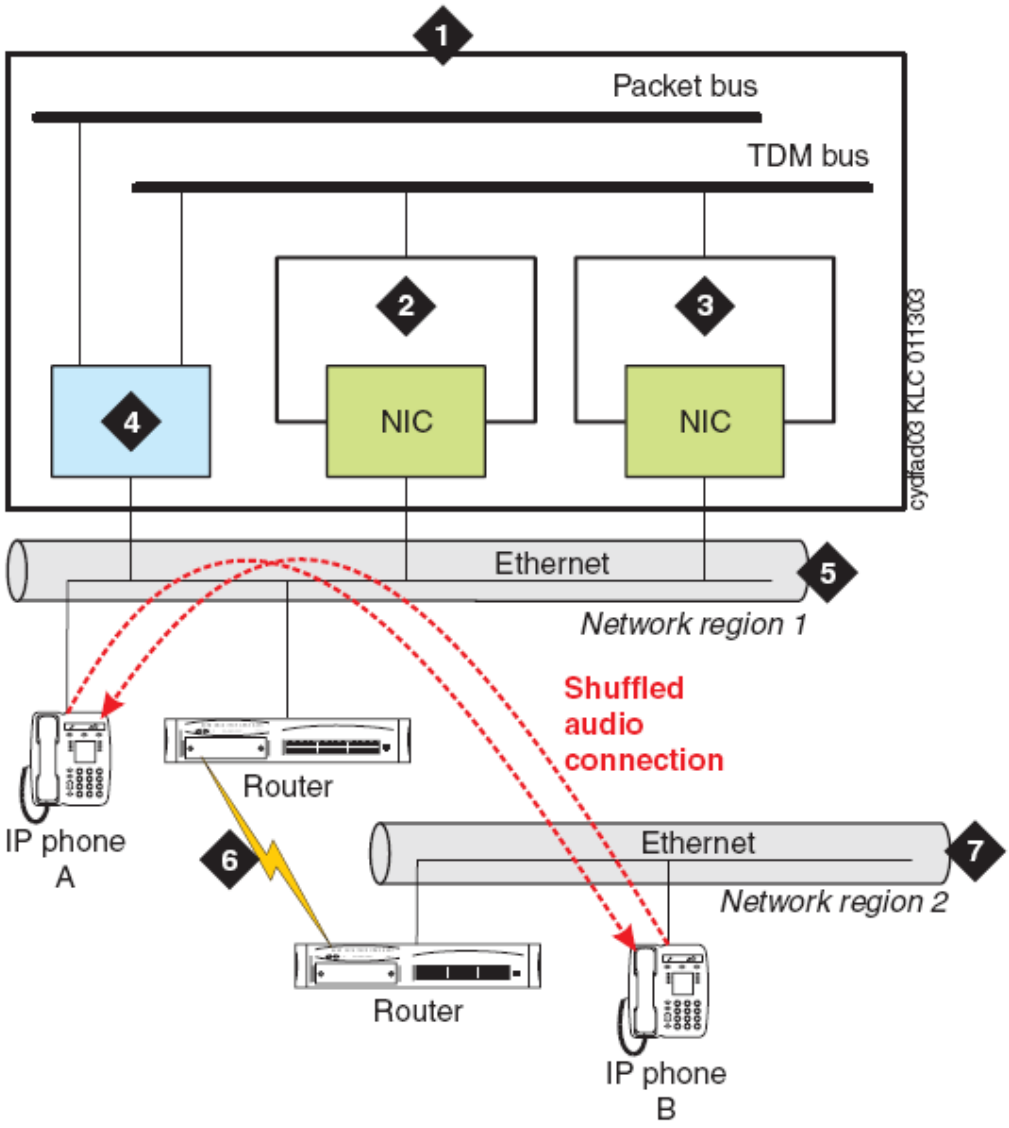


Figure 7: Shuffled audio connection between IP endpoints in different network regions

Number	Description
1	Avaya server
2	TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit pack
3	TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit pack
4	TN799 Control LAN (C-LAN) circuit pack

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 85 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.

Hairpinned audio connections

Hairpinning means rerouting the voice channel that connects two IP endpoints. After rerouting, the voice channel goes through the TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit packs in IP format. Without hairpinning, the voice channel goes through the TDM bus.Communication Manager provides only shallow hairpinning. Only the IP and Real Time Protocol (RTP) packet headers are changed as the voice packets go through the TN2302AP or TN2602AP circuit pack. For hairpinning, both endpoints must use the same codec. The codec is a circuit that takes a varying-voltage analog signal through a digital conversion algorithm to the corresponding digital equivalent or vice versa. Throughout this section, the word hairpin refers to shallow hairpinning.

Criteria for hairpinning

Communication Manager uses the following criteria to determine whether to hairpin the connection:

- A point-to-point voice connection exists between two endpoints.
- The endpoints are in the same network region, or in different, interconnected regions.
- A single TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack serves both endpoints.
- The endpoints use a single, common codec.
- The endpoints are administered for hairpinning. For shuffled IP calls to use a public IP address by default, set the **Direct IP-IP Audio Connections** field to `y`.
- If the **IP Audio Hairpinning** field is `y`, but during registration, if the endpoint indicates that it cannot support hairpinning, the call cannot be hairpinned. In some instances, the **IP Audio Hairpinning** field is `n`, but during registration, the endpoint indicates that it can support

hairpinning. Even in these instances, calls to that endpoint cannot be hairpinned, giving precedence to the endpoint administration.

- Communication Manager determines whether a shuffled audio connection is possible.
- Both endpoints can connect through the same TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack.

Example of a hairpinned call

Hairpinned audio connections:

- Set up within approximately 50 milliseconds.
- Maintain the Real-Time Protocol (RTP) header. For example, the time stamp and packet sequence number.
- Do not require volume adjustments on Avaya endpoints. However, non-Avaya endpoints might require volume adjustment after the hairpinned connection is established.

Figure 8: Hairpinned audio connection between two IP endpoints in the same network region on page 88 is a schematic of a hairpinned audio connection between two IP endpoints in the same network region.

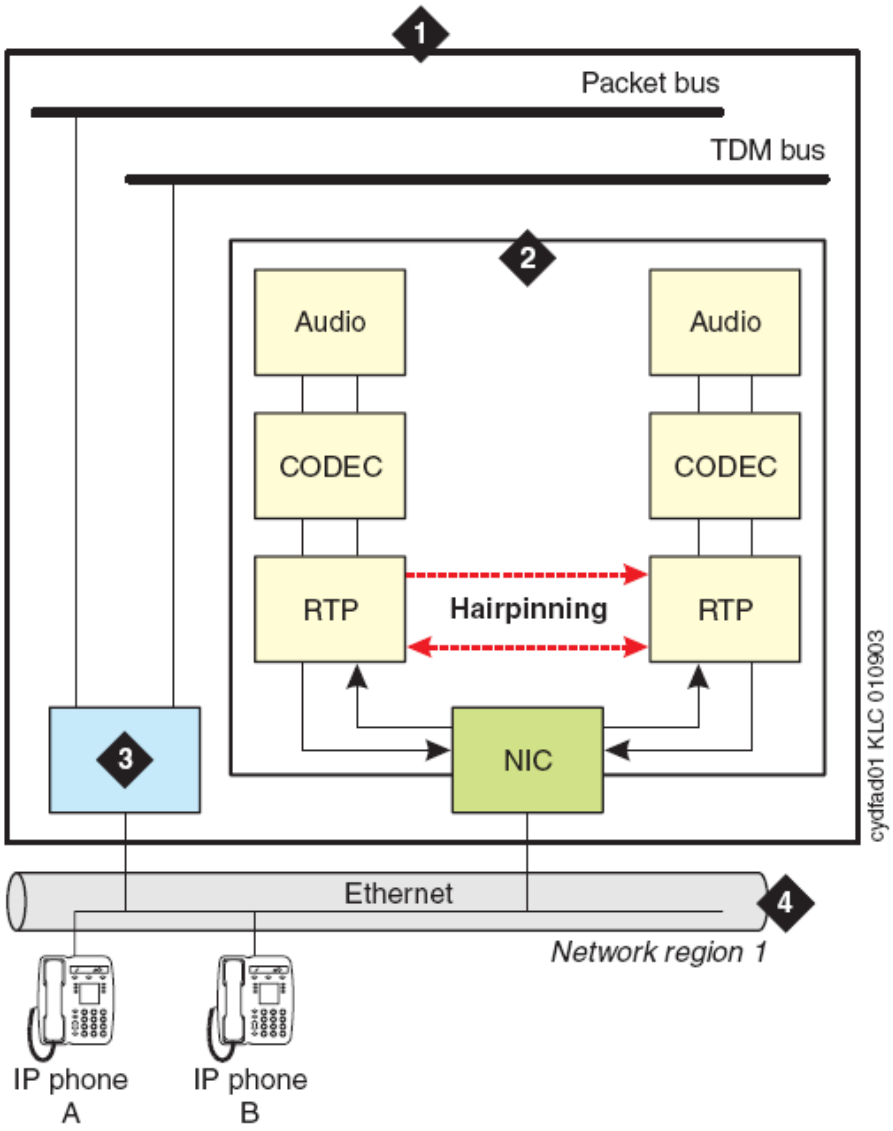


Figure 8: Hairpinned audio connection between two IP endpoints in the same network region

Name	Description
1	Avaya server
2	TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit pack
3	TN799 Control LAN (C-LAN) circuit pack
4	LAN/WAN segment administered in Communication Manager as network region 1

Figure 8: Hairpinned audio connection between two IP endpoints in the same network region on page 88 shows that hairpinned calls bypass the TN2302AP or TN2602AP codec freeing those

resources for other calls. The necessary analog or digital conversions occur in the common codec in each endpoint.

Causes of a redirected hairpinned call

A hairpinned connection is broken and the call is rerouted over the TDM bus when:

- A third party is conferenced into a hairpinned call.
- A tone or announcement must be inserted into the connection.

Determining which TN2302AP or TN2602AP circuit pack is hairpinning

About this task

When a TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack hairpins calls, the TN2302AP or TN2602AP yellow LED is on steady. You cannot easily identify all the extension numbers that are hairpinning through a particular TN2302AP or TN2602AP circuit pack. However, you can determine which TN2302AP or TN2602AP circuit pack a particular extension is using for hairpinning.

Procedure

1. At the SAT, type **`status station extension`** and press `Enter`.

   The system displays the Station screen for that extension.
2. Scroll to page 4 of the report.
3. In the AUDIO CHANNEL section, check the value in the **Audio** field in the Switch Port column.

   If no port is listed in the Audio field, then the call is hairpinned.

Hairpinning and shuffling administration interdependencies

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

Note:

To use hairpinning or 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.

Important:

Encryption must be disabled for hairpinning to work because encryption requires the involvement of resources that are not used in the shallow hairpinning connection. However, encryption and shuffling can work together.

Table 5: Hairpinning and shuffling administration

Administration screen	Required customer options	Other interactions
Station	IP StationsRemote Office	Hairpinning is unavailable if the **Service Link Mode** field on Station screen is `permanent`. 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.
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 fields for hairpinning and 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 hairpinning or shuffling. See Determining whether an endpoint supports shuffling on page 84.

Note:

Direct Media

Communication Manager supports 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 hairpinning and shuffling in network regions on page 95

Preparing to enable Direct Media

Procedure

1. Ensure that the call originator is SIP.

   If the call originator is not SIP, Communication Manager does not apply 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 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.

  It can be a portal to the gatekeeper, such as a C-LAN, or the gatekeeper itself, processor Ethernet such as an S8300D Server or S8300E.
- Gateway: The Avaya device that is handling media conversion between TDM and IP. The device can be a MedPro board, G700 VoIP Media Module, or any of the following branch gateways:
  - G450
  - G430
  - G350
  - G250

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.

Hairpinning and shuffling

You can administer shuffled and hairpinned connections:

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

Checklist for administering hairpinning and shuffling

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

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

No.	Task	Description	✔
1	Administer hairpinning and shuffling for the system from the Feature-Related System Parameters screen.	See Administering hairpinning and shuffling at the system-level on page 94.	
2	Administer hairpinning and shuffling for the network region level from the Network Region screen.	See Inter-network region connection management on page 95.	
3	Administer hairpinning and shuffling for IP trunks from the Signaling Group screen.	See Administering H.323 trunks for hairpinning and shuffling on page 97.	
4	Administer hairpinning and shuffling for IP endpoints from the Station screen.	See Administering IP endpoints for hairpinning and shuffling on page 98.	

Administering hairpinning and 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** and **IP Audio Hairpinning** fields do not display.

About this task

You can administer hairpinning or shuffling as a systemwide 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. In the **IP Audio Hairpinning** field, type `y`.

4. Save the changes.

Internetwork region connection management

Shuffling and hairpinning 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 hairpinning and 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 hairpinning and 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. Administer the **IP-IP Direct Audio** fields:

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.

The following values are permitted for both fields:

- **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.

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*, 03-300509 and *Avaya Aura® Solution Design Considerations and Guidelines*, 03-603978.

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*, 03-602878.

   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 TN799 C-LAN or TN2032 IP Media Processor resources among network regions.

   Note:

   Use the `list ip-codec-set` command for a list of codecs.

4. Save the changes.

Related links

IP codec sets on page 125
Hairpinning and shuffling administration interdependencies on page 89

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 125.

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 (intraregion) and between or among (interregion) network regions. If the endpoint and the TN2302AP or TN2602AP are in the same region, the administered intraregion codec set is chosen. If the endpoint and the TN2302AP or TN2602AP are in different regions, the administered interregion 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 TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 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 hairpinning and 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 hairpinning and 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. In the **IP Audio Hairpinning** field, type `y`.

4. 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 89

Administering IP endpoints for hairpinning and 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

Shuffle or hairpin is independently administered for each endpoint on the Station screen. The specific station types that you can administer for hairpinning or 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. In the **IP Audio Hairpinning** field, type `y`.

4. 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 89

IP station administration for dual-connect

IP stations administered for dual-connect cannot shuffle calls if the extension numbers have differing values in the following fields:

- **Direct IP-IP audio Connections**
- **IP-IP Audio Hairpinning**

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 TN2302AP Media Processor or TN2602AP IP Media Resource 320. For these IP audio signals, the circuit pack 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 TN2302AP or TN2602AP circuit pack to insert loss into the signal coming from the IP telephone. The circuit pack 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 hairpinned or 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 categorized as follows:

- Category A: Vintage products that use older chip technologies and have slight operational differences from category B devices. Category A devices include MM760, TN2302, G250, G350, and G700.
- Category B: Products that use newer chip technologies. Category B products include TN2602, 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:

For category A devices, modulation and demodulation reduces the number of simultaneous calls that a device can handle.

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. For example, with the Pass-through mode on G700 Branch Gateway, you can make 64 simultaneous fax or modem calls instead of only 16 with Relay. The capability applies to only category A devices.

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 sychronized clocks.

T.38

In the T.38 mode, the gateway DSP devices or the G650 VoIP boards 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*, 555-245-205.

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.

Note:

The G650 gateway does not support the RFC 4040 feature. G430 and G450 gateways support the RFC 4040 feature. The gateway in the network region must support the RFC 4040 feature for Communication Manager to connect RFC 4040 calls.

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*, 03-602878.

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 Codec Set screen.

2. Assign each codec set to the appropriate network region.
3. Assign the network region to the appropriate devices:
   - TN2302AP or TN2602AP.
   - Avaya G250, G350, G430, G450, or G700 branch gateways
4. **(Optional)** Administer internetwork region connections if the TN2302AP or TN2602AP resources are shared among administered network regions.

Related links

Defining IP interfaces on page 66
IP codec sets on page 125
IP network regions on page 128
Manually interconnecting the network regions on page 139

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 110.

- 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 7: Bandwidth for FAX, modem, and TTY calls over IP networks on page 109 .

- 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 Simplex and Duplex servers, certain hardware vintages and firmware versions are required for the TN2302AP or the TN2602AP circuit pack. See *Avaya Aura® Communication Manager Minimum Firmware/Hardware Vintages* at http://support.avaya.com.
  - For the G700 and G350 branch gateways, the respective firmware version 22.14.0 and VoIP firmware Vintage 40 or later to support Communication Manager 2.2 are required. An MM760 Media Module with firmware Vintage 40 or later can be used for more VoIP capacity. To check the latest firmware, go to http://support.avaya.com .
  - For Avaya S8300D Servers, Avaya G250 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.

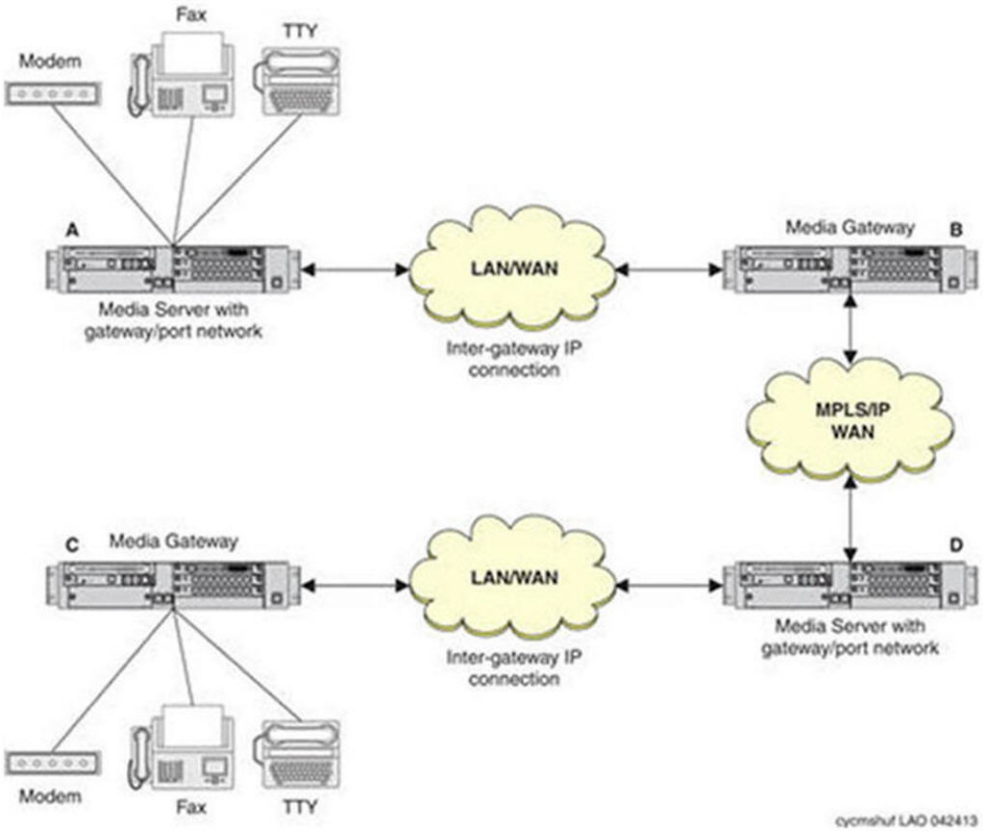


Figure 9: Shuffling for FAX, modem, and TTY calls over IP

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 6: 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

Table continues…

Mode	Maximum rate	Comments
		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.
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-codec-set screen. **Note:** The T.38 with fallback to G.711 Pass-through feature only works over SIP trunks.

Table continues…

Mode	Maximum rate	Comments
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.
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.

Table continues…

Mode	Maximum rate	Comments
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.
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 transcodings 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 7: 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.

Note:

Encrypted calls reduce Digital Signal Processing (DSP) capacity by 25% compared to nonencrypted calls. DSP capacity reduction does not apply to category B devices. Encryption does not reduce capacity on these platforms.

Encryption is applicable as shown in the following table.

Table 8: 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	(Y)	N	Duplicate Packets
TTY Pass-through	Y	Y	Y	RTP (RFC2198)
TTY Relay	Y	Y	Y	RFC2198
T.38 FAX Standard	(Y)	(Y)	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 112.

AES encryption in FAX Relay is available only with Avaya equipment (TN2302) with the correct vintages.

The T.38 Fax standard does not support encryption. An enhancement of the T.38 standard enables AES and AEA encryption only with Avaya equipment (TN2302) with the correct vintage.

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:

- Avaya Aura® Media Server
- TN2602AP Media Resource 320
- MM760
- VoIP Media Modules and on-board VoIP engines as follows:
  - G350 Branch Gateway
  - G250 Branch Gateway
  - G430 Branch Gateway
  - G450 Branch Gateway

The following gateway platforms support SRTCP and AES-256:

- VOIP Media Modules on gateways 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-codec-set 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 `change ip-codec-set n`, where *n* is the ip codec set number.

   The system displays the IP Codec Set 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 5: 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® Solution Design Considerations and Guidelines*, 03-603978.

For more information about implementing QoS, see the White Paper, *Avaya IP Voice Quality Network Requirements (LB1500-02)*, at http://www.avaya.com/master-usa/en-us/resource/assets/whitepapers/lb1500-02.pdf.

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 9: User complaints and their causes

Complaint	Possible causes and links to information
'Talking over' the far end	• Packet delay and loss • Echo

Table continues…

Complaint	Possible causes and links to information
	• 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® Solution Design Considerations and Guidelines*, 03-603978.

Echo

Echo occurs when you hear your own voice reflected back with a slight delay. Echo can originate from the following sources:

- Electrical: From unbalanced impedances or cross talk.
- Acoustical: Introduced by the speakerphone or room size.

Echo path delay is the round-trip time from when a voice packet enters the network to the time that the voice packet returns to the originator. In general, calls over a WAN normally have a longer echo path delay compared to calls over a LAN.

Note:

VoIP does not cause echo. However, significant amounts of delay or jitter associated with VoIP can make imperceptible echo perceptible.

Echo cancellers

Echo cancellers minimize echo by comparing the original voice pattern with the received patterns and canceling the echo if the patterns match. However, echo cancellers do not provide optimum performance in the following conditions:

- When the round-trip delay from the echo canceller to the echo reflection point is longer than the buffer time for the nonechoed signal. During the buffer time, the nonechoed signal is buffered in the echo canceller memory.

  The larger the memory of the echo canceller, the longer the signal is held in the buffer. Therefore, with a larger memory for the echo canceller, the number of packets that the canceller can compare in the allotted time is maximized.
- During Voice Activity Detection (VAD), which monitors the level of the received signal:
  - An energy drop of at least 3dB weaker than the original signal indicates echo.
  - An energy level of 3dB greater indicates far end speech.

Echo cancellers do not work well over analog trunks and with speaker phones with volume controls that result in strong signals. Although VADs can greatly conserve bandwidth, overly aggressive

VADs can cause voice clipping and reduce voice quality. VAD administration is done on the station screen for the IP telephone.

Analog trunks in IP configurations need careful network balance settings to minimize echo. A test tone of known power is sent out. The return signal measured to determine the balance setting, which is critical for reducing echo on IP calls across these trunks.

Echo cancellation plans for TN464HP and TN2464CP circuit packs

The following summarizes the echo cancellation plans that are available exclusively for the TN464HP and TN2464CP circuit packs. For echo cancellation plans that are available for the TN464GP and TN2464BP circuit packs, see *Echo cancellation plans for TN464GP/TN2464BP circuit packs*.

Echo Cancellation Configuration 1

Plan 1 is the recommended choice. The plan has comfort noise generation and residual echo suppression turned on. During a single talk, background noise and residual echo from the distant station can be suppressed and replaced with comfort noise. The comfort noise substitution reduces the perception of background noise pumping, as observed by the talker. In this plan, the EC direction is chosen to cancel the echo of the talker. Because this plan turns on comfort noise and echo suppression, the plan is similar to EC plans 8 and 9 for the TN464GP/TN2464BP circuit packs.

Echo Cancellation Configuration 2

Plan 2 has comfort noise generation turned off and residual echo suppression turned on. This plan can work well in a quiet background environment. In a noisy background environment, the talker can hear background noise pumping or clipping. In this case, EC direction is chosen to cancel the echo of the talker. This plan can be a good compromise for a small percent of users, who prefer silence during the residual echo suppression periods. The plan turns off comfort noise and turns on residual suppression. Therefore, Echo Cancellation Configuration 2 for the TN464HP and TN2464CP circuit packs is similar to EC configurations 1-6 for the TN464GP and TN2464BP circuit packs.

Echo Cancellation Configuration 3

Plan 3 has comfort noise generation and residual echo suppression turned off. This configuration can be a good choice only if EC plans 1 and 2 do not satisfy the user. Situations that require configuration 3 must be rare. For example, the user does not care for the sound of comfort noise nor the pumping or clipping of background noise. Using this configuration, you can hear natural sound from the earpiece. However, the user can hear residual echo during training periods, or during all times if echo is sufficiently high and residual echo is always present. Convergence can be very slow. In Echo Cancellation Configuration 3 for TN464HP and TN2464CP circuit packs, comfort noise and residual suppression are turned off. Therefore, the configuration is similar to EC configuration 7 for the TN464GP and TN2464BP circuit packs.

Echo cancellation plans for TN464GP/TN2464BP circuit packs

Communication Manager supports several echo cancellation (EC) plans for the TN464GP and TN2464BP circuit packs.

Note:

An EC configuration setting can be changed in real time. The change takes effect immediately. You can change the setting on the DS1 Circuit Pack screen. You need not busyout or release

the circuit pack. You can change the EC configuration setting without disruption to existing calls. You can immediately hear the effect of the change.

Important:

When TN2302AP or TN2602AP circuit packs and TN464GP/TN2464BP circuit packs are used for a call, the echo canceller on TN2302AP or TN2602AP is turned off. The echo canceller on the TN464GP/TN2454BP is used instead, because it has the greater echo canceller.

The following summarizes the echo cancellation plans that are available for the TN464GP/TN2464BP circuit packs. For echo cancellation plans that are available exclusively for the TN464HP/TN2464CP circuit packs, see Echo cancellation plans for TN464HP/TN2464CP circuit packs.

Echo Cancellation Configuration 1 – Highly Aggressive Echo Control

This configuration can control strong echo from a distant party. Echo Cancellation Configuration 1 and Echo Cancellation Configuration 4 provide the most rapid convergence in detecting and correcting echo at the beginning of a call. The initial echo fades faster than the other settings, in a fraction of a second, regardless of the loudness of the voice of the talker. EC Configurations 1 and 4 are the same except for loss. EC Configuration 1 has 6dB of loss and EC 4 has 0dB of loss. Therefore, EC Configuration 1 is a good choice for consistently high network signal levels. EC Configuration 1 can cause low-volume complaints and complaints of clipped speech utterances. These complaints occur particularly in doubletalk conditions, that is, when both parties speak simultaneously. Because EC Configuration 1 relies on echo suppression to control echo, pumping the background noise of the distant party can occur and lead to complaints. Before Communication Manager Release 2.0, EC Configuration 1 was the default configuration.

The 6dB of loss in EC Configuration 1 is in one direction. The direction of loss depends on the setting of the **EC Direction** field on the DS1 Board screen. If the direction is set to `inward`, then the 6dB of loss is inserted in the path out from the board towards the T1/E1 circuit. Conversely, if the setting is `outward`, then the 6dB of loss is inserted into the path from the T1/E1 circuit towards the TDM bus.

Echo Cancellation Configuration 2 – Aggressive, Stable Echo Control

This configuration is nearly identical to EC Configuration 1, except that it does not inject an extra 6dB of signal loss. Also, convergence of the echo canceller is slower in EC Configuration 2, but more stable than that provided by EC Configuration 1. If EC Configuration 1 diverges during doubletalk conditions, use EC Configuration 2 instead of EC Configuration 1. Divergence is noticeable by the sudden onset of audible echo. Because the echo canceller converges somewhat slower, some initial echo can be noticeable at the beginning of a call, while the system is training. EC Configuration 2 can cause complaints of clipped speech utterances, particularly during doubletalk. Because EC Configuration 2 relies on echo suppression to control echo, pumping of the background noise of the distant party background noise can occur and lead to complaints.

Echo Cancellation Configuration 3 – Aggressive, Very Stable Echo Control

This configuration is nearly identical to EC Configuration 2, but is more stable. Because the echo canceller converges somewhat slowly, some initial echo can be noticeable at the start of a call. EC Configuration 3 can cause complaints of clipped speech utterances, particularly during doubletalk. Because EC Configuration 3 relies on echo suppression to control echo, pumping of the background noise of the distant party background noise can occur and lead to complaints.

Echo Cancellation Configuration 4 – Highly Aggressive Echo Control

This configuration is identical to EC Configuration 1, but does not provide the 6dB loss option as described for EC Configuration 1. All other comments from EC Configuration 1 apply to EC Configuration 4. EC Configuration 4 can cause complaints of clipped speech utterances, particularly during doubletalk. Because EC Configuration 4 relies on echo suppression to control echo, pumping of the background noise of the distant party background noise can occur, and lead to complaints.

Echo Cancellation Configuration 5 – Very Moderate, Very Stable Echo Control

This configuration departs significantly from EC Configurations 1 – 4. The echo canceller is slower to converge and is stable after converging. Some initial echo can be heard at the beginning of a call. EC Configuration 5 does not, in general, lead to complaints of clipped speech or pumping of the background noise of the distant party.

Echo Cancellation Configuration 6 – Highly Aggressive Echo Control

This configuration is identical to EC Configuration 4. However, reliance on the echo suppressor to control echo is half that of EC Configuration 4. As a result, EC Configuration 6 does not clip speech as much as EC Configuration 4. However, EC Configuration 6 can cause somewhat more audible echo, particularly at the start of a call. Some pumping of the background noise of the distant party background noise can be perceptible.

Echo Cancellation Configuration 7 – Extremely Moderate and Stable Echo Control

This configuration provides very stable and transparent control of weak to low-level echoes. For connections having audible echo at the start of a call, the residual echo can linger for several seconds as the echo canceller converges.

Echo Cancellation Configuration 8 – Aggressive, Very Transparent Echo Control 1

This configuration provides aggressive control of echo at the start of a call and more moderate control during the call. Unlike all earlier settings, EC Configuration 8 uses comfort noise injection to match the noise level of the distant-party speech signal. The effect is one of echo canceller transparency in which complaints of clipped speech or noise pumping are few to none. To many people, EC Configuration 8 and EC Configuration 9 are indistinguishable.

Echo Cancellation Configuration 9 – Aggressive, Transparent Echo Control 2

This configuration is nearly identical to EC Configuration 8, but provides somewhat more residual echo control at a slight expense of transparency. To many people, EC Configuration 8 and EC Configuration 9 are indistinguishable.

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 IP Media Processor 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. VLAN administration is at two levels:

- Circuit pack-level administration on the IP-Interfaces screen. See *Defining IP interfaces (C-LAN, TN2302AP, or TN2602AP Load Balanced)*.
- Endpoint-level administration on the IP Address Mapping screen.

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.

   The IP address must be a 32-bit address with four decimal numbers, each in the range 0-255.

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

   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 nonmasked rightmost bits. The address becomes the stored From address.
   - Mask is applied to the **TO IP Address** field, putting 1s in the nonmasked 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, C-LAN, or Media Processor boards.

   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 Codec Set screen. The codecs on the IP Codec Set 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 Codec Set 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 hairpinning and shuffling in network regions on page 95

Administering an IP Codec set

Procedure

1. Type `change ip-codec-set` *set#* and press `Enter`.

   The system displays the IP Codec Set 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. Save the changes.
15. Type `list ip-codec-set` and press `Enter`.

    The system lists all codec sets on the CODEC Set screen.
16. 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 include Media Processor and C-LAN circuit packs. In this context, IP endpoint refers to IP stations, IP trunks, and G150, G250, G350, G430, G450, and G700 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*, 03-300509.

Note:

For more information about using network regions, with examples, see the application note Network Regions for Avaya MultiVantage™ Solutions - A Tutorial, at: http://www.avaya.com/gcm/master-usa/en-us/resource/assets/applicationnotes/advantages_of_implem.pdf. 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.avaya.com/master-usa/en-us/resource/assets/applicationnotes/netw-region-tutorial.pdf.

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
Region	Network Region number, 1–2000.
Location	Blank or 1–2000. If you leave the field blank, the system obtains the location from the cabinet containing the C-LAN 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.
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

Table continues…

Name	Description
	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.
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	

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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.
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.

Call Admission Control

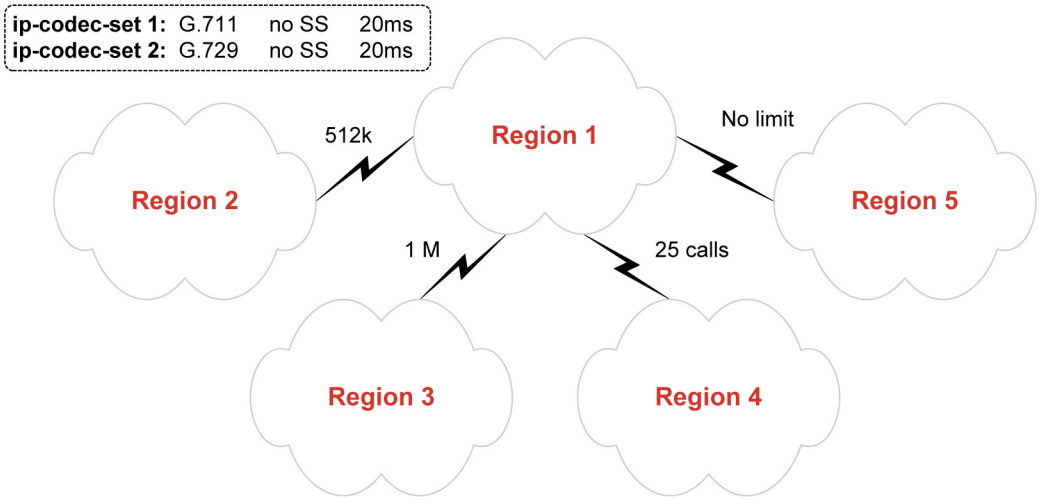
Call Admission Control (CAC) is a feature to set a limit on the bandwidth consumption or number of calls between network regions.

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*® *Solution Design Considerations and Guidelines*, 03-603978.
- 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.



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    n
 2    2     y    NoLimit                                        n    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    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   _____                                                          ___
```

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.

Network Region Wizard

The AvayaNetwork Region Wizard (NRW) is a browser-based wizard that supports IGAR, CAC, and codec set selection for interconnected region pairs. For a system with several network regions, the wizard can configure the system for best IP performance and save time for the personnel provisioning the system.

Through a simplified, task-oriented interface, the NRW guides you through the steps required to define network regions and set all necessary parameters. With NRW, provisioning of multiple IP network regions is simple and quick. For example, NRW is beneficial while provisioning Call Admission Control through Bandwidth Limits (CAC-BL) for large distributed single-server systems that have several network regions. NRW is especially valuable for provisioning systems with numerous network regions, for which administration using the System Access Terminal (SAT) scales poorly.

NRW provisioning tasks include:

- Specification and assignment of codec sets to high-bandwidth or intraregion LANs and lower-bandwidth or interregion WANs.
- Configuration of IP network regions, including all intraregion settings, and interregion administration of CAC-BL for interregion links.
- Ongoing network region administration by the customer, Avaya technicians, and Business Partners to accommodate changes in the customer network following cutover.
- Assignment of VoIP resources, such as C-LANs, TN2302/TN2602 circuit packs and Gateways, and endpoints to IP network regions.

NRW simplifies and expedites network region provisioning by:

- Using algorithms and heuristics based on graph theory to reduce the repetitive manual entry in SAT to configure codecs and CAC-BL for interregion links. With SAT, the number of interregion links that must be configured by the user does not scale well. With the NRW, the number of region pairs that require manual administration increase linearly with the number of regions.
- Providing OVA of widely applicable default values for codec sets and intraregion parameter settings. Users can customize the OVA with the default values that users prefer.

- Running on any Internet browser supported by the Avaya Integrated Management (IM) product line. NRW uses browser capabilities to offer user-friendly prompting and context-sensitive online help.

For the NRW Job Aid and worksheet, see http://support.avaya.com/avayaiw. This standard IM support tool is delivered with every Linux-based Communication Manager system.

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 TN799DP C-LAN and TN2302AP IP Media Processor 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 interregion 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 nolimit.

For more information about using network regions, see *Network Regions for Avaya MultiVantage™ Solutions - A Tutorial* at: http://www.avaya.com/gcm/master-usa/en-us/resource/assets/applicationnotes/advantages_of_implem.pdf. For more information about configuring network regions in Communication Manager, see *Avaya Aura® Communication Manager Network Region Configuration Guide*, at: http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/netw-region-tutorial.pdf. For information about using the Network Region Wizard, see *Network Region Job Aid, 14-300283* 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 10: 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 interregion 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.

Port network to network region mapping for circuit packs other than IP circuit packs

Existing IP Media Processor or Resource Modules, for example, the MedPro, C-LAN, and VAL, have assigned IP network regions. The new mapping from cabinet to IP Network Region does not override this administration.

The critical non-IP boards of interest are the trunk circuit packs over which IGAR calls are routed. In some instances, the system cannot establish an IP connection between two Port Networks or media gateways (PNs or MGs). Then, the system tries to establish an IGAR trunk connection between the two PNs or MGs. The system tries to use trunks in the specific PN/MG requested. However, because Communication Manager does not require every PN or MG to have PSTN trunks, you must get trunks from another PN or MG. The system can only get trunks from a PN or MG in the same network region as the one in which the original request was made. Thus, with Communication Manager, customers must be able to associate a port network with a network region.

Note:

Cabinets connected through a center stage switch (CSS) are required to be in network region 1.

```
display cabinet 1                                                SPE B

                                CABINET
 CABINET DESCRIPTION
                  Cabinet: 1
            Cabinet Layout: five-carrier
              Cabinet Type: processor
   Number of Portnetworks: 1
    Survivable Remote EPN? n
                 Location: 1               IP Network Region: 1
          Cabinet Holdover: A-carrier-only
                      Room: 1K26_____    Floor: _______  Building: 22_____

CARRIER DESCRIPTION
  Carrier       Carrier Type        Number      Duplicate

     C        port_____________     PN   01
     B        processor________     PN   01
     A        processor________     PN   01
     X        fan______________
     D        dup-sw-node______     SN   01        01E
     E        switch-node______     SN   01        01D
```

Figure 11: IP network region field on cabinet screen to map PNs to network regions

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.

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 12: IP network region status screen

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 G700.
2. At the P330-x(super)# prompt, type `set spantree help` and press `Enter`.

   The system displays the Set spantree commands screen.

   Figure 13: Set Spantree commands on page 145 shows the full set of Spanning Tree commands.

```
P330-1(super)# set spantree help
Set spantree commands:
--------------------------------------------------------------------------------
set spantree enable                     Set spanning tree enable.
set spantree disable                    Set spanning tree disable.
set spantree max-age                    Set spanning tree bridge max-age.
set spantree hello-time                 Set spanning tree bridge hello-time.
set spantree forward-delay              Set spanning tree bridge forward-delay.
set spantree version                    Set spanning tree version.
set spantree tx-hold-count              Set spanning tree bridge tx-hold-count.
set spantree priority                   Set spanning tree bridge priority
set spantree default-path-cost
                        Set spanning tree default-path-cost.

P330-1(super)# set spantree version help
Set spantree version commands:
--------------------------------------------------------------------------------
Usage: set spantree version <version>
<version> - the version of the spanning tree protocol
            common-spanning-tree - compatible with ieee802.1D standard
            rapid-spanning-tree - compatible with ieee802.1W standard

P330-1(super)#
```

   Figure 13: 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

Most of the Avaya 96x1 SIP and H.323 phones support AES128 encryption standard.

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 Codec Set 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 Codec Set screen is hidden and functions as if `none` is selected.

About this task

On the IP Codec Set 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 `change ip-codec-set` *number* and press `Enter`.

   The system displays the IP Codec Set 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 130

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
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.

Table continues…

Name	Description
	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 Codec Set 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 10: Media Encryption interactions on page 152

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 10: Media Encryption interactions on page 152

Table 10: 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 TN2302AP IP Media Processor circuit pack receives the encrypted voice stream, it 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.
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
- Administrable IPSI Socket Sanity Timeout
- 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® Solution Design Considerations and Guidelines*, 03-603978.

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 14: Avaya Policy Manager application sequence on page 154, you can see how Avaya Policy Manager works.

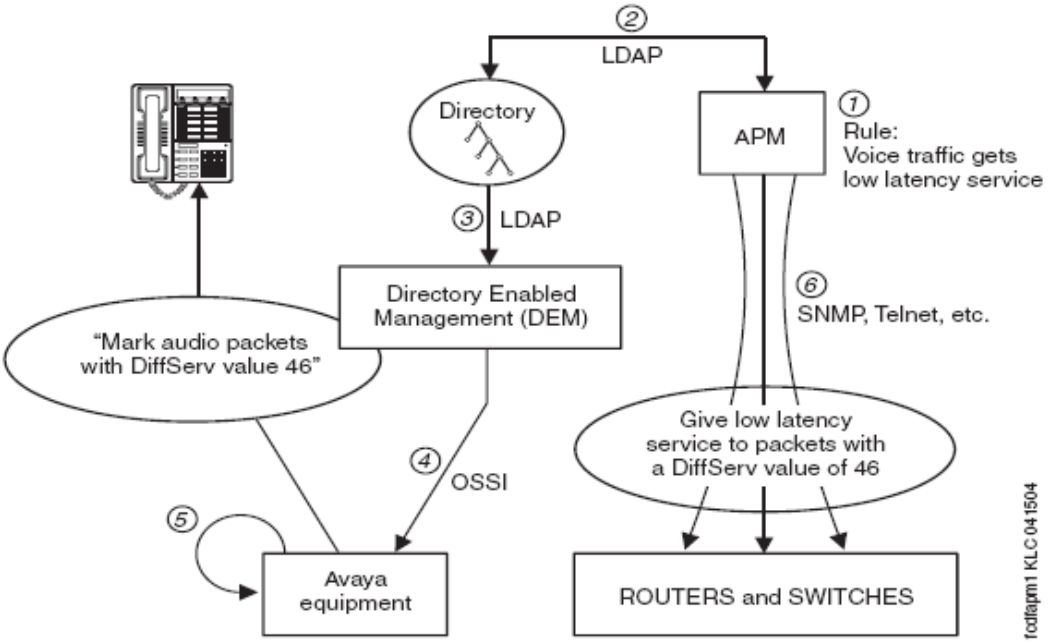


Figure 14: Avaya Policy Manager application sequence

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, Media Processor, C-LAN, 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 TN799DP C-LAN circuit packs. Link Recovery can connect to a circuit pack within the configuration of the original server or to a survivable remote server.

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 6.0 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 6.0, while the gateway is required to have the gateway firmware available at the time of the Communication Manager 6.0 release.

Existing branch gateways are the targets.

For each gateway, the following administration must be performed:

- Adding Recovery Rule to Gateway screen.
- Scheduling the autobfallback 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 3.0, 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.

G250 interworking

When calls are made on the gateway controlled by Standard Local Survivability (SLS), the G250, G350, G430, and G450 work as any other survivable remote. Using the administration and dial analysis plan, the SLS can establish local calls from a:

- Local station to local station with analog or registered IP

- Local station to local analog two-way CO trunks

While operating in SLS mode, the G250 attempts to reregister with the primary controller on the MGC list of the G250. When the gateway can reregister with the primary controller, the gateway unregisters with SLS and reregisters with the primary controller. In terms of reregistration with the primary controller, the auto fallback to primary feature works identically for the G250 SLS and survivable remote servers in the G350 or G700.

Note:

The connection maintaining aspects of this feature are unavailable on the G250 for this release.

G350 interworking

The G350 firmware loads use the Object Identifier (OID) that has the longer Non-Standard Data format in the registration message. This format is only backward compatible to Communication Manager 2.0 loads. Older loads respond with a protocol error as the cause for the rejection of the new registration message. Given that the G350 was only introduced in the Communication Manager 2.0 time frame, G350 is not backwards compatible with previous Communication Manager releases.

In a startup scenario, version information is exchanged between Communication Manager and the gateway. If the Communication Manager load is for a version earlier than Communication Manager 3.0, then the auto fallback mechanism remains disabled for the gateway. Any subsequent registration with a primary controller, from the MGC list, that is running release Communication Manager 3.0 results in the auto fallback feature being enabled for the gateway.

The gateway can send a registration message to an older primary call controller only in specific cases. Registration to an older primary controller occurs only when the primary controller is downgraded while the gateway receives service from a survivable remote server. In this case, the gateway receives a protocol error that can be used to send a registration message consistent with Communication Manager 2.0. Downgrading to a version earlier than Communication Manager 2.0 with a G350 can result in the G350 not being able to register at all.

G700 interworking

The G700 Branch Gateway still uses the same OID as when it was originally deployed. The OID available for the G350 was not ported to the G700. The auto fallback to primary feature requires that all G700s running the Communication Manager compliant firmware load use the OID format. The Non-Standard Data (NSD) expansion with the OID is used to carry the context count.

If the gateway receives any of the following errors in response to a registration message, then the gateway sends the original OID registration message before the expansion of the NSD:

- 284: NSD OID invalid
- 283: SD OID wrong length
- 345: NSD wrong length - for Communication Manager 1.3 and earlier systems

Although unnecessary for this feature, the gateway responds to any of these protocol errors by attempting to register with the lowest common denominator registration message. The new gateways are backward compatible with older releases. This change only applies to the G700.

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 250 applies a specific recovery rule to that numbered gateway.

   An S8300D Serverand S8300E support up to 50 gateways, and a standalone server supports up to 250 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*, 03-300431 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 S8300D Server, you can administer up to 50 screens, while for standalone servers, you can administer up to 250 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 S8300D Server and S8300E server • Up to 250 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 15: 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.

Administrable IPSI Socket Sanity Timeout

The IPSI Socket Sanity Timeout provides a link-bounce interval between Communication Manager and the IPSI to provide resiliency during short network outages. During normal operations, Communication Manager monitors the connection to an IPSI by using a heartbeat sent by the IPSI every second. If a heartbeat is missed and Communication Manager does not receive any other data from the IPSI, an IPSI sanity failure occurs. The number of IPSI sanity failures are counted and compared to the value set by an administrator for the IPSI Socket Sanity Timeout. The administered value must be between 3 to 15 seconds. Communication Manager uses the administered value to determine how long to wait for communication to the IPSI to be restored before a recovery action is initiated. If the value for IPSI Socket Sanity Timeout is correctly engineered, the IPSI is less prone to warm starts and resilient to short network outages.

If the IPSI Socket Sanity Timeout is greater than three, the port network (PN) can handle only less than three sanity failures. If more than three sanity failures occur, the PN is placed in a suspended state. An event is logged recording the transition of the PN from an available state to a suspended state. All messages sent from call processing to the PN and vice versa are delayed until communication resumes. The PN does not go into a suspended state if IPSI Socket Sanity Timeout is equal to three or if less than three sanity failures occur.

If communication is restored between the server and the IPSI before the value set for the IPSI Sanity Timeout elapses, call processing resumes. If the timer expires before communication resumes, the socket between the server and the IPSI is torn down and Communication Manager attempts to reconnect to the IPSI. If the attempts to reconnect are successful, the PN resets. The type of reset depends on the length of the outage. If communication is restored within 1 minute, a warm restart is performed, but after 1 minute, a cold restart is performed.

Customers might have a value for IPSI Socket Sanity Timeout set by Avaya Services, other than the default 3 second value. When such customers upgrade to the latest release of Communication Manager, the value set by Avaya Services is carried over during the upgrade.

Note:

The value administered for the IPSI Socket Sanity Timeout does not affect the survivable core server service timer.

The IPSI Socket Sanity Timeout is administered on page one of the system-parameters ipserver-interface form in the **IPSI Socket Sanity Timeout** field. The range for this field is 3 to 15 seconds with the default set at 3 seconds.

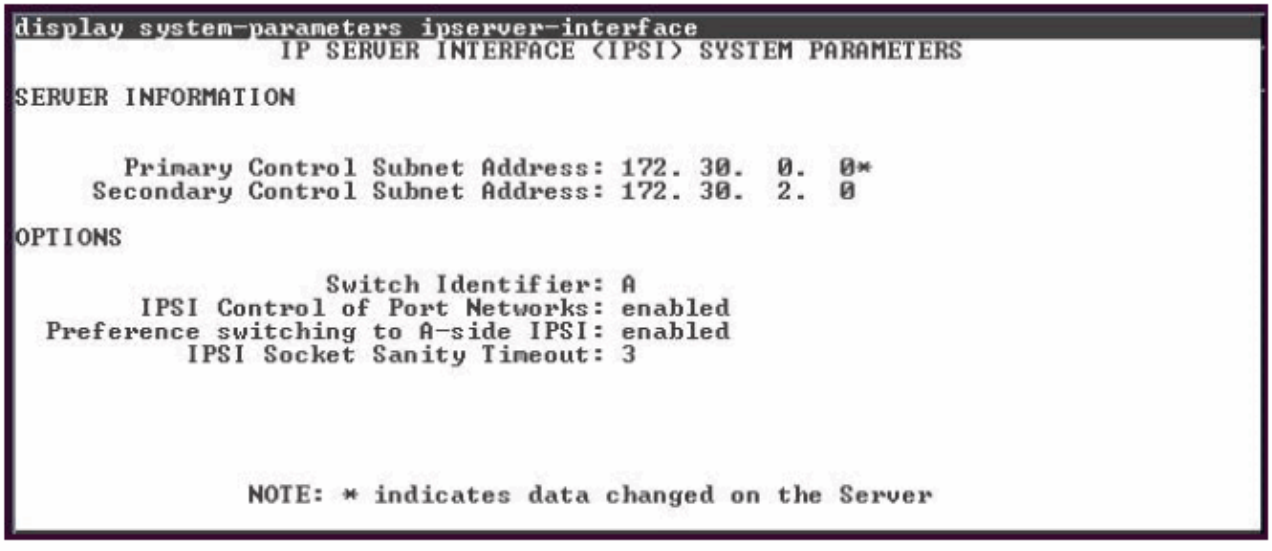


Figure 16: system-parameters ipserver-interface

Survivable core servers

The survivable core servers provide survivability to port networks by putting backup servers in various locations in the network of the customer. The backup servers supply service to port networks when the main server or connectivity to the main Communication Manager server is lost. Survivable core servers offer full Communication Manager functionality when in survivable mode, provided adequate connectivity exists to other Avaya components, for example, endpoints, gateways, and messaging servers.

When designing a network to support survivable core servers, consider the following:

- Survivable core servers can only control port networks that the servers can reach over an IP-connected network.

  Survivable core servers connected on a public IP network for an enterprise cannot control port networks connected to control network A or B. This control is possible when control networks A or B are exposed to the public IP network through control network on the Customer LAN (CNOCL).
- Multiple survivable core servers can be deployed in a network. An enterprise can deploy one or more survivable core servers on the public network. The enterprise can also deploy another server on control networks A and B to back up port networks attached to the respective networks.

  However, when port networks register with different survivable core servers, system fragmentation can occur. Therefore, you must establish adequate routing patterns at a particular location to be able to make calls where needed.
- Survivable core servers register to the main servers through a C-LAN. Each survivable core server must be able to communicate with a C-LAN to download translations from the main server. The file synchronization process uses the following ports:
  - UDP/1719: Survivable core server registers with the main server.
  - TCP/21873: Main server sends translations to the survivable remote servers. This port is used for releases earlier than Release 3.0.
  - TCP/21874: Main server sends translations to the survivable core server. This port is used for Release 3.0 and later, and also for survivable remote server translations.

The gateway cannot distinguish between registration through a C-LAN or registration to an S8300D Server. When a gateway registers through the C-LAN IP address of the primary call controller, the gateway is not necessarily registered with the true primary call controller. The port network that houses the C-LAN is under the control of a survivable core server. However, the gateway cannot determine whether the registration is with a survivable core server.

When the traditional port network migrates to the primary call controller, the gateway loses the H.248 link and uses the Link Loss Recovery algorithm. The auto fallback to primary feature is used only if the gateway drops the connection and registers with a survivable remote server. Survivable core server migration must occur only if the port network is reasonably certain to return to the primary call controller. The port network must return to the primary call controller, so the gateway returns to the same C-LAN interface. The Link Loss Recovery feature then performs a context audit

with the primary controller and determines that the primary call controller is not aware of the gateway. The controller in this case issues a warm start request to the gateway, or potentially different instructions if connection preservation is active simultaneously. The auto fallback feature is not affected by survivable core server.

For more information about survivable core servers, see *Avaya Aura® Communication Manager Survivable Options*, 03-603633.

Improved port network recovery from control network outages

When the network fails, IP-connected port networks have disproportionately long outages from short network disruptions. The improved port network recovery feature now ensures less downtime during IP network failures for customers that use IP connected port networks.

The feature lessens the impact of network failures by:

- Improving TCP recovery times that increase the IPSI-PCD socket bounce coverage time. This time is now increased from the current 6 to 8 seconds for the actual network outage to closer to 10 seconds. Results vary based on traffic rates.
- Modifying the PKTINT recovery action after a network outage to entail a warm interrupt instead of a PKTINT application reset hardware interrupt. This change prevents H.323 IP telephones from having to reregister or have sockets regenerated. This change also minimizes recovery time from network outages in the range of 15 to 60 seconds.

With this feature, you can monitor the IPSI-PCD socket and identifying and troubleshoot network-related problems.

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

During network outage, bearer connections are preserved only for stable calls already in progress. A call with an established talk path between the parties in the call is considered stable. Call control is unavailable during the network outage, which means that any call in a changing state is most likely not preserved.

Some examples of calls in changing state include:

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

- Calls in ACD queues
- Calls in vector processing

Further, no change in the state of a preserved call is possible. So, features such as conference or transfer are unavailable on the preserved calls. Button pushes are not recognized. When the feature is requested by users, the request is denied. In a conference call, if a party drops, the entire call is dropped.

The following additional improvements are available with this feature:

- Improved TCP Recovery Time.
- Increased IPSI Local Buffering to prevent data loss.
- Reduced escalation impact from 15 to 60 seconds by using warm interrupt of PKTINT instead of PKTINT application reset hardware interrupt.
- Reduced escalation impact for 60 to 90 seconds by extending the PN cold reset action from 60 seconds to 90 seconds.
- Decreased minimum value of No Service Timer in survivable core server from 3 minutes to 2 minutes to reduce local customer outage during prolonged network outage.
- List measurements for the PCD-PKTINT socket for improved troubleshooting.

These improvements are available with the introduction of a warm interrupt of the PKTINT instead of reset in the 15 to 60 seconds range. These changes are also influenced by the optional extension of the PN cold reset from 60 to 120 seconds.

Port Network Recovery Rules screen field descriptions

```
change system-parameters port-networks                          Page 2 of 2

                    PORT NETWORK RECOVERY RULES


 FAILOVER PARAMETERS                        FALLBACK PARAMETERS

 No Service Time Out Interval (min): 5              Auto Return: no

    PN Cold Reset Delay Timer (sec): 60
```

Figure 17: PN Cold Reset Delay Timer

Name	Description
No Service Time Out Interval (min)	No Service Time Out Interval in minutes. This value can rangè from 2 to 15 minutes.
PN Cold Reset Delay Timer (sec)	PN Cold Reset Delay Timer in seconds. This value can range from 60 to 120 seconds. The default value is 60 seconds

Survivability

Reducing the minimum time of No Service Time Out Interval in the survivable core server from 3 to 2 minutes improves customer availability.

Chapter 6: Resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® Solution Design Considerations and Guidelines, 03-603978	Describes all the components that work with Communication Manager.	Solution Architects, Sales Engineers, Support Personnel
Implementation		
Avaya Aura® Communication Manager Survivable Options, 03-603633	Describes the survivable options. Also contains information about designing, configuring, administering, maintaining, and troubleshooting survivable options.	Implementation Engineers, Support Personnel
4600 Series IP Telephone Installation Guide, 555-233-128	Describes the equipment and resources required for installation, and how to set local administrative options.	Implementation Engineers, Support Personnel
Avaya one-X Deskphone Edition 9600 Series IP Telephone Installation and Maintenance Guide, 16-300694	Describes how to install and maintain the 9600 Series IP Telephone product line and troubleshoot telephone problems.	Implementation Engineers, Support Personnel
Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide, 16-601438	Describes the implementation of Communication Manager, DHCP, HTTP/HTTPS servers for 1600 Series IP Telephones, a Local Area Network (LAN), or a Web server.	Implementation Engineers, Support Personnel
Maintenance and Troubleshooting		
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers	Describes the commands for Communication Manager.	Solution Architects, Implementation Engineers, Support Personnel
Administration		

Table continues…

Title	Description	Audience
Administering Avaya Aura® Communication Manager, 03-300509	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Solution, Architects, Implementation, Engineers, Support, Personnel
4600 Series IP Telephone LAN Administrator Guide, 555-233-507	Describes the administration of DHCP and TFTP servers to support the Avaya 4600 Series IP Telephones.	Implementation Engineers, Support Personnel
Avaya one-X Deskphone Edition 9600 Series IP Telephones Administrator Guide, 16-300698	Describes the administration of Communication Manager, DHCP, HTTP/HTTPS servers for 9600 Series IP Telephones, a Local Area Network (LAN), or a Web server.	Sales Engineers, Implementation Engineers, Support Personnel
Understanding		
Avaya Aura® Communication Manager Hardware Description and Reference, 555-245-207	Describes the hardware devices that can be incorporated in a Communication Manager telephony configuration.	Sales Engineers, Solution Architects, Support Personnel

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
Understanding	
1A00234E	Avaya Aura® Fundamental Technology
AVA00383WEN	Avaya Aura® Communication Manager Overview
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
2007V	What is New in Avaya Aura® 7.0
2009V	What is New in Avaya Aura® Communication Manager 7.0
2011V	What is New in Avaya Aura® System Manager & Avaya Aura® Session Manager 7.0
2009T	What is New in Avaya Aura® Communication Manager 7.0 Online Test
2013V	Avaya Aura® 7.0 Solution Management
5U00060E	Knowledge Access: ACSS - Avaya Aura® Communication Manager and CM Messaging Embedded Support (6 months)
Implementation and Upgrading	
4U00030E	Avaya Aura® Communication Manager and CM Messaging Implementation
ATC00838VEN	Avaya Media Servers and Implementation Workshop Labs
AVA00838H00	Avaya Media Servers and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop Labs
2012V	Migrating and Upgrading to Avaya Aura® 7.0
Administration	
AVA00279WEN	Communication Manager - Configuring Basic Features
AVA00836H00	Communication Manager Basic Administration
AVA00835WEN	Avaya Communication Manager Trunk and Routing Administration
5U0041I	Avaya Aura® Communication Manager Administration
AVA00833WEN	Avaya Communication Manager - Call Permissions
AVA00834WEN	Avaya Communication Manager - System Features and Administration
5U00051E	Knowledge Access: Avaya Aura® Communication Manager Administration

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.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://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.

Appendix A: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) if any software update. For example, a PCN must accompany a service pack or a update that must be applied universally.Avaya issues product-support notice (PSN) when there is no update, service pack, or release fix, but the business unit or services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a work around for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.

   Note:

   If the Avaya Support website displays the login page, enter your SSO login credentials.
2. On the top of the page, click **DOCUMENTS**.
3. On the Documents page, in the **Enter Your Product Here** field, enter the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select the appropriate filters as per your search requirement. For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   Note:

   You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new services packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to the Avaya Support Web Tips and Troubleshooting: E-Notifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#.
2. Set up e-notifications.

   For detailed information, see the **How to set up your E-Notifications** procedure.

Index

Numerics

1600-series IP Telephones 79
4600-series IP phone, configuration files 80
4600-series IP Telephones 78
802.1p/Q 123
9600-series IP telephones 79
96x1–series IP telephones 78

A

adding
  Recovery Rule on Media Gateway screen 159
administering
  C-LAN and IP Media Processor circuit packs 63
  DPT 137
  DS1 circuit pack 44
  endpoints for IP address mapping 124
  gateways 59
  H.323 trunks 67
  H.323 trunks for hairpinning and shuffling 97
  hairpinning and shuffling at system level 94
  hairpinning and shuffling in network regions 95
  IP codec set 126
  IP endpoints for hairpinning and shuffling 98
  media encryption for IP codec sets 148
  media encryption for signaling groups 150
  MM710 media module 44
  network performance parameters 144
  network region 143
  SRTP 113
  Telecommuter telephone 75
  trunk group for echo cancellation 46
administrable loss plan 86
administration
  H.323 Trunk 62
  H.323 Trunks 62
  IP telephones 80
  UDS1 circuit pack 44
adminster and select
  codecs 96
affected features
  increase in locations 14
alarm
  settings mismatch 57
assigning
  IP node names 65
auto fallback to primary 23
  feature operation 156
Avaya courses 169

B

bandwidth 122
bandwidth limitation 139
bearer duplication
  requirements 53
Best Service Routing (BSR) 66

C

CAC 133
call admission control 133
Call Admission Control 139
checklist
  administering hairpinning and shuffling 94
circuit packs
  control LAN (C-LAN) interface 18
  duplicated bearer connections 30
  TN2602AP 29
C-LAN 18
  circuit pack TN799DP 46
  installation 47
C-LAN board
  IP addressing techniques 47
  physical addressing 47
C-LAN connectivity
  cable connection 48
connecting switches 15
connection management
  inter-network region 95
Connection Preservation 22
converged networks 42
CPM feature 23
create
  SIP trunk signaling group 61
creating
  H.323 trunk signaling group 68

D

default gateway 48
default node 48
defining
  IP network region 129
determining
  endpoint support for shuffling 84
  whether media encryption is enabled 148
digital telephone calls
  data types 11
  DCS signaling data 11
disabling
  spanning tree 145
DPT 17

DPT and IGAR
comparison ... 17
DS1 circuit pack
administration ... 44
echo cancellation ... 44
duplex IP-PNC duplicated control network
architecture ... 34
duplex IP-PNC single control network
architecture ... 32
Duplex server
reliability options ... 26
Duplicated bearer ... 37
Duplicated server
duplicated control ... 34, 36
IP-PNC ... 36
Duplicated server IP-PNC ... 34
duplicated TN2602AP circuit packs ... 66
duplicated TN-2602AP circuit packs ... 29

E

echo cancellation ... 118
MM710 media module ... 44
plans (TN464GP and TN2464BP circuit packs) ... 119
trunks ... 45
echo cancellation plans
TN464HP and TN2464CP circuit packs ... 119
echo path delay ... 118
ELS ... 23
enabling
spanning tree ... 145
encryption, media ... 147
endpoint
gatekeeper settings ... 50
Enhanced Local Survivability (ELS) ... 23
Enterprise Survivable Servers ... 24
ESS ... 24

F

failure conditions ... 152
Fax over IP
administration ... 102
overview ... 99
Super G3 fax machine ... 125
Fax pass through
bandwidths ... 109
considerations for configuration ... 103
encryption ... 110
Fax relay
bandwidths ... 109
considerations for configuration ... 103
encryption ... 110
field description
media encryption ... 149
field descriptions
IP Network Region ... 130

G

G250 Media Gateway ... 24, 157
G700/G350 Media Gateways ... 18, 158
gateway
default ... 48
generating CPN ... 72

H

H.248
link loss recovery ... 154
H.248 auto fallback to primary ... 23, 155
H.248 link recovery ... 23
H.323 clear channel over IP ... 99
H.323 link recovery ... 23
H.323 Trunk
administration ... 62
hairpinned call
example ... 87
hairpinned call redirection
causes ... 89
hairpinning and shuffling ... 94
administration interdependencies ... 89
direct media ... 81
supported endpoints ... 82
supported hardware ... 82
hairpinning audio connections
criteria ... 86
hardware interface ... 18

I

iClarity ... 76
IGAR ... 16
pair-wise administration ... 140
implementing QoS ... 116
improved port network recovery
network outage ... 164
INADS line
restrictions for usage ... 21
increase in locations
affected features ... 14
installing
C-LAN ... 47
C-LAN cables ... 47
TN2302AP, TN2602AP, and TN799DP circuit packs ... 80
Inter-Gateway Alternate Routing ... 16
internetwork region connections ... 139
interregion usage
status ... 142
interworking
G250 ... 157
G350 ... 158
G700 ... 158
IP codec sets, administering ... 125
IP interface ... 66

IP interfaces 66
IP Media Resource 320
firmware download 54
IP network regions 128
IP-PNC 25
reliability options 26
IP-PNC networks 15
IP-PNC simplex server
architecture 28
IPSI QoS parameters
default settings 57
IPSI socket sanity timeout 161
IP Softphone
administration 74
Alternate Gatekeeper 49
IP station administration
dual-connect 98
IP telephone 77
administration 80
IP telephones 74
IP trunks 60

J

jitter 18
jitter buffers 146

L

LAN security
system architecture 21
legal notice .....
link recovery 23
load balanced TN2602AP circuit packs 66
LSP 23

M

media encryption 147
FAX, modem, and TTY 110
feature interactions 152
license file 148
limitations 147
SRTP 110
support 147
Media Gateway Report screen 161
Migrate H.248 MG to primary
options 160
Mixed PNC
mixed reliability with IP-PNC example 39
MM710 media module
administration 44
MM710 T1/E1 Media Module 43
MM760
supported branch gateways 59
voice compression 59
MM760 VoIP Media Module 18, 58
Modem over IP
administration 102
overview 99
Modem pass through
bandwidths 109
considerations for configuration 103
description 105
encryption 110
rates 105
Modem relay
bandwidths 109
considerations for configuration 103
description 105
encryption 110
rates 105
monitor
network performance 153
MultiVOIP gateways 15

N

NAT 91
network
converged 11
dedicated 11
IP 11
nondedicated 11
Network Address Translation 91
NAPT 92
NAT and H.323 issues 92
NAT Shuffling feature 93
types of NAT 92
network management 153
network recovery 153
Network regions 12
network regions, IP 128
node
default 48
node names, assigning 64
non-IP boards
Port network to network region mapping 141
No Server Time Out Interval
impact 166
NRW 138

O

older gateway loads 159
overview
converged networks 42

P

pass-through mode 100
PCN notification 171

PCNs 171
PE
recommended firmware 20
support on Survivable Core server 20
PE interface 19
Per Hop Behaviors 123
port address translation (PAT) 92
port network
reliability 25
port network connectivity
duplex IP-PNC 30
Duplicated server
IP-PNC 34, 36
mixed reliability with IP-PNC example 39
simplex server 27
Port Network Recovery Rules
field descriptions 165
preparing
before enabling Direct Media 91
PSN notification 171
PSNs 171

Q

QoS 18
voice quality administration 122
QoS parameters 64
QoS policies 153
Quality of Service (QoS) 18
Quality of Service policies 153

R

Rapid Spanning Tree 16
recovery rules
defining 159
Relay mode 100
reliability
dependant factors 25
reviewing
network region administration 143
RSVP 123

S

S8300E 18, 80, 93, 143, 159, 160
Service Observing 151
service-observing
IP stations 98
Session Initiation Protocol (SIP) 60
setting
network performance thresholds 111, 144
shuffled audio connection
within a network region 83
shuffled connections 121
shuffling
criteria 82
different network regions 85
signaling data 16
signaling group 67, 72
signal loss
IP endpoint 99
signing up
PCNs and PSNs 172
Simplex server
IP-PNC 27
reliability options 26
SIP 64K Data 102
SIP session refresh
failure handling 22
SIP trunks 60
SLS 24
spanning tree protocol (STP) 16
SRTP 114
SRTP media encryption 112
for FAX, modem and TTY 110
Standard Local survivability 24
STP 16
Super G3 fax machine 125
support 170
supported platforms 113
survivability 22, 153
Survivable Core servers 24
Survivable Remote servers 23
System Parameters Media Gateway Automatic Recovery Rule
field description 160

T

T.38 101
T.38 fax
bandwidths 109, 110
considerations for configuration 103
overview 99
T.38 fax standard mode 108
telephone, IP 77
TN2302AP 50
TN2302AP circuit pack
determine whether hairpinning 89
TN2302AP IP Media Processor
jitter buffers 51
test ports 51
TN2302AP Media Processor
hairpinning 51
TN2312BP (IPSI) 18
TN2312BP IPSI 54
description 55
firmware 55
TN2602AP circuit pack
administer for duplication 66
administer for load balancing 66
determine whether hairpinning 89

TN2602AP circuit packs
bearer duplication 52
enable bearer duplication 52
load balancing 52, 53
TN2602AP features 53
TN2602AP IP Media Resource 320 ..... 18, 66
capacity options 51
TN2602AP IP Media Resource 320 circuit pack
I/O adapter 54
TN799 (C-LAN)
Alternate Gatekeeper 18, 49
TN802B MAPD IP Interface Assembly 18
training 169
trunk group 70
trunks
H.323 62
SIP 60
TTY over IP
administration 102
overview 99
TTY pass through
bandwidths 109
considerations for configuration 103
description 105
encryption 110
rates 105
TTY relay
bandwidths 109
considerations for configuration 103
description 105
encryption 110
rates 105

U

UDS1 circuit pack, administration 44
Universal DS1 (UDS1) circuit pack 43
USA DCP levels
loss 99
User Datagram Protocol (UDP) 163
User Datagram Protocol ports 146

V

V.150.1 Modem Relay 101
VAD 118
verifying
customer options for H.323 trunking 63
videos 170
video signaling 114
viewing
encryption status 151
Virtual Local Area Networks 124
Voice Activity Detection 118
voice degradation
causes 117
factors 116
VoIP hardware 43