Administering Network Connectivity on Avaya Aura™ Communication Manager

555-233-504
Issue 15
Sept 2010

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Websites referenced within this site or documentation(s) 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 this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Website: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by the said Avaya reseller and not by Avaya.

Licenses

The software license terms available on the Avaya Website, http://support.avaya.com/licenseinfo/ are applicable to anyone who downloads, uses and/or installs Avaya software, purchased from Avaya Inc., any Avaya affiliate, or an authorized Avaya reseller (as applicable) under a commercial agreement with Avaya or an authorized Avaya reseller. 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 authorized reseller, and 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 End User a license within the scope of the license types described below. 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 End User. “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. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

- Designated System(s) License (DS):
  End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, 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.
- Named User License (NU):
  End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use 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 (for example, 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):
  Customer 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”). (See Third-party Components for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. 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.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Website: http://support.avaya.com/Copyright.

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 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:

http://www.support.avaya.com/.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to:securityalerts@avaya.com.

Trademarks

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

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, 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(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.

All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Website: http://www.avaya.com/support.

Contact Avaya Support

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

Contents

Chapter 1: Networking overview

This chapter provides background information to help you understand and use the information in this book. Telephony delivered over digital networks capitalizes on the flexibility of technology itself, and can be implemented in a variety of ways. Users might find that they need to reference only a portion of the information in this book. Other readers might need most of its information before understanding how to tailor a telephony network to suit their needs.

About “network” terminology

The Communication Manager *network* can contain multiple interconnected servers and all of the equipment, including data networking devices, controlled by those servers. Such equipment may be geographically dispersed among a variety of sites, and the equipment at each site may be segregated into distinct logical groupings, referred to as *network regions*. A single server system has one or more *network regions*. Each *network region* is a logical grouping of endpoints, including stations, trunks, and media gateways. In cases where one server is insufficient for controlling all of the equipment, multiple systems can be networked together. So, one or more *network region(s)* comprise a *site*, and one or more sites comprise a *system*, which in turn is a component of a *network*.

For the purposes of this book and to clarify what we mean by the word, consider these uses of the word “network”:

- Businesses often have a “corporate network,” meaning a Local Area Network (LAN) or a Wide Area Network (WAN), over which they distribute E-mail, data files, run applications, access the Internet, and send and receive fax and modem calls.

  We use *non-dedicated* to describe this type of network and the traffic that it bears. This means that the network is a heterogeneous mix of data types.

- When a non-dedicated network carries digitized voice signals along with other data types, we call this a *converged* network, because it is a confluence of voice and non-voice data.
- Network segments that exclusively carry telephony traffic are *dedicated*, since they carry only telephony-related information.
- When a digital network carries telephony and non-telephony data in a packet-switched (TCP/IP), instead of a circuit-switched (TDM) environment, we call this an *IP network*.

About digital telephone calls

A digital phone call consists of voice (bearer) data and call-signaling messages. Some transmission protocols require sending signaling data over a separate network, virtual path, or “channel,” from the voice data. The following list describes the data that are transmitted between switches during a phone call:

- Voice (bearer) data — digitized voice signals
- Call-signaling data — control messages
    - Set up the call connection
    - Maintain the connection during the call
    - Tear down the connection when the call is finished
- Distributed Communications System (DCS) signaling data

  Distributed Communications System (DCS) allows two or more communications switches to be configured as if they were a single switch. DCS provides attendant and voice-terminal features between these switch locations. DCS simplifies dialing procedures and allows transparent use of some Communication Manager features. Feature transparency means that features are available to all users on DCS regardless of the switch location.

About network regions

A network region is a group of IP endpoints that share common characteristics and resources. Every IP endpoint on the Communication Manager system belongs to a network region.

By default, all IP endpoints are in network region 1. If left that way, all IP endpoints would all share the same characteristics defined by network region 1 and use the same resources. But in many cases, this is not sufficient to allow for certain differences that may be based upon location or network characteristic, and therefore multiple network regions should be configured.

The most common of these cases are:

- One group of endpoints requires a different CODEC (COder-DECoder) set than another group.

  This could be based on requirements related to bandwidth or encryption.
- Calls between separate groups of endpoints require a different codec set than calls within a single group of endpoints, again based on requirements related to bandwidth or encryption.
- Specific C-LAN or MedPro or other resources must be accessible to only a specific group of endpoints.

- One group of endpoints requires a different UDP port range or QoS parameters than another group.
- One group of endpoints reports to a different VoIP Monitoring Manager server than another group.

Somewhat related to network regions is the concept of locations. The *location* parameter is used to identify distinct geographic locations, primarily for call routing purposes. In other words, the location parameter is used primarily to ensure that calls access the proper trunks, based on the origin and destination of each call.

Establishing inter-switch trunk connections

Connected switches enable people within an enterprise to communicate easily with one another, regardless of their physical location or the particular communications server they use. Inter-switch connections also provide shared communications resources such as messaging and Call Center services.

Switches communicate with each other over trunk connections. There many types of trunks that 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 transmit 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 provide connections between switches in a private network.

These and other common trunk types are described in the Administering *Avaya Aura™ Communication Manager*, 03-300509.

Interconnecting port networks

Note:

See Chapter 2: Port network configurations on page 19 for detailed examples of IP-connected (IP-PNC) networks.

Networking branch offices

For Communication Manager environments, the G430 voice over IP gateways (Multi-Tech Systems, Inc.) provide distributed networking capabilities to small branch offices of large corporations. MultiVOIP extends the call features of a centralized Avaya server and provides local office survivability to branch offices of up to 15 users using analog or IP phones.

For more information, see: http://www.multitech.com/PARTNERS/Alliances/Avaya/.

Control networks

Control networks are the networks over which Communication Manager exchanges signaling data with the port networks through the IPSI circuit packs and with the H.248 Media Gateway through the server Processor Ethernet.

Enabling spanning tree protocol (STP)

Spanning Tree Protocol (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is to always leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) can lead to a complete cessation of all traffic.

However, STP is slow to converge after a network failure, and slow to allow a new port into the network (~50 sec by default).

A modified version of STP, Rapid Spanning Tree converges faster than the earlier STP, and enables new ports much faster (sub-second) than the older protocol. **Rapid Spanning Tree** works with all Avaya equipment, and is *recommended* by Avaya.

Inter-Gateway Alternate Routing (IGAR)

For single-server systems that use the IP-WAN to connect bearer traffic between port networks or media gateways, Inter-Gateway Alternate Routing (IGAR) provides a means of alternately using the PSTN when the IP-WAN is incapable of carrying the bearer connection. IGAR may request that bearer connections be provided by the PSTN under the following conditions:

- The number of calls allocated or bandwidth allocated via Call Admission Control-Bandwidth Limits (CAC-BL) has been reached.
- VoIP RTP resource exhaustion in a MG/PN is encountered.
- A codec set is not specified between a network region pair.

- Forced redirection between a pair of network regions is configured.

IGAR takes advantage of existing public and private-network facilities provisioned in a network region. Most trunks in use today can be used for IGAR. Examples of the better trunk facilities for use by IGAR would be:

- Public or Private ISDN PRI/BRI
- R2MFC

IGAR provides enhanced Quality of Service (QoS) to large distributed single-server configurations.

In general, 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, use H.323 or SIP trunks for IGAR. To carry the bearer traffic through H.323 or SIP trunks, administer the following fields:

- Set the **IGAR Over IP Trunks** field on the **Feature-Related System Parameters** screen.
- If appropriate for your network, set the **Incoming Dialog Loopbacks** field on the **SIP Signaling Group** screen.

Dial Plan Transparency

Dial Plan Transparency (DPT) preserves the dial plan when a media gateway registers with a Survivable Remote server or when a 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.

Network quality management

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

- *Delay:* Significant end-to-end delay may result in echo and talker overlap.
- *Packet Loss:* Under peak network loads and periods of congestion, voice data packets may be dropped.
- *Jitter (Delay Variability):* Jitter results when data packets arrive at their destination at irregular intervals as a result of variable transmission delay over the network.

Note:

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

- Chapter 5: Voice and Network quality administration on page 127

  - *Avaya Application Solutions: IP Telephony Deployment Guide*, 555-245-600

About VoIP-transmission hardware

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

For more information about these and other 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 Setting up VoIP hardware on page 39.

- TN799DP control LAN (C-LAN) interface

  The 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. (With the Communication Manager release 5.0 and beyond, IP connectivity between servers and H.248 Media Gateway can be established directly through server Processor Ethernet and there is no need for C-LAN). For more information on Processor Ethernet and setting up processor Ethernets, see *Administering Avaya Aura™ Communication Manager, 03-300509.*

- TN2312BP IP Server Interface (IPSI)

  The IPSI provides for the transport of control messages between servers and port networks.

- TN2302AP IP Media Processor and TN2602AP IP Media Resource 320

  The TN2302AP and TN2602AP provide high-capacity VoIP audio access to the switch for local stations and outside trunks.

- H.248 media gateways

  The H.248 media gateways include the G700, G250, G350, G430, G450, and IG550.

  The H.248 media 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.
  - Survivable Remote server backup for a remote server.

- MM760 VoIP Media Module

  The MM760 VoIP Media Module is a clone of the G700 motherboard VoIP engine. The MM760 provides an additional 64 VoIP channels in the G700.

Processor Ethernet (PE)

Much like a C-LAN board, Processor Ethernet 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 (that is, the so-called “native NIC”). No additional hardware is needed to implement PE. Processor Ethernet uses the PROCR IP-interface type.

During the configuration of a server, the PE is assigned to a Computer Ethernet (CE). The PE and the CE share the same IP address, but are very different in nature. The CE interface is a native computer interface while the PE interface is the logical appearance of the CE interface within Communication Manager software. The interface that is assigned to the PE can be a control network or a corporate LAN. The interface that is selected determines which physical port the PE uses on the server. For more information on 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. On a Survivable Remote server, the H.248 and the H.323 fields default to a ***yes*** on the **IP Interface Procr** screen, to allow the registration of H.248 gateways and H.323 endpoints using the Processor Ethernet interface.

In Communication Manager release 5.2 and later, H.248 Media Gateway and H.323 endpoint registration on a Survivable Core server is allowed if you administer the **Enable PE for H.248 Gateways** and **Enable PE for H.323 Endpoints** fields on the **Survivable Processor** screen on the main server. Therefore the H.248 and H.323 fields on the **IP Interface Procr** screen of the Survivable Core server display the values that you administered.

⚠ **Important:**

Both the Survivable Core server and the Survivable Remote server require the use of the Processor Ethernet interface to register to the main server. Do not disable the Processor Ethernet interface on a Survivable Core server or a Survivable Remots server.

Support for Processor Ethernet and Port Networks on an Survivable Core Server

In Communication Manager Release 5.2 and later, the capabilities of Survivable Core servers are enhanced to support connection of IP devices to the Processor Ethernet interface as well as to C-LAN interfaces located in G650 (port network) gateways.

An Survivable Core server can use its Processor Ethernet interface to support IP devices such as H.248 Media Gateways, H.323 Media Gateways, IP Adjuncts, IP telephones, IP trunks, and SIP trunks. The Survivable Core server can optionally control port networks (G650 Media Gateways) through IPSI at the same time. When there are no port networks in the configuration, Survivable Core server may provide the equivalent benefit of a Survivable Remote server. The Survivable Core server can be duplicated, providing additional redundancy to the survivability of the system.

For Processor Ethernet on duplex servers to work, you must assign the Processor Ethernet interface to the PE Active server IP Address (IP-alias) 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 Survivable Core server registers to the C-LAN on the main server, the C-LAN must have IP connectivity to the LAN assigned to the NIC used for Processor Ethernet on the ESS.
- If the Survivable Remote server or Survivable Core server registers to the Processor Ethernet on the main server, the Processor Ethernet on the main server must have IP connectivity to the LAN assigned to the NIC used for Processor Ethernet on the Survivable Core server.

Firmware for optimal performance

Processor Ethernet on duplex servers works ively only when the H.248 gateways and IP telephones are on the most current release of firmware.

Avaya recommends that you 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; 9670 as of firmware relase 3.1, 9808 9611, 9621, and 9641(all releases), any future 96xx models that support TTS (Time to Service) will work optimally.
- 4601+, 4602SW+, 4610SW, 4620SW, 4621SW, 4622SW, and 4625SW Broadcom telephones with firmware R 2.9 SP1 or later.

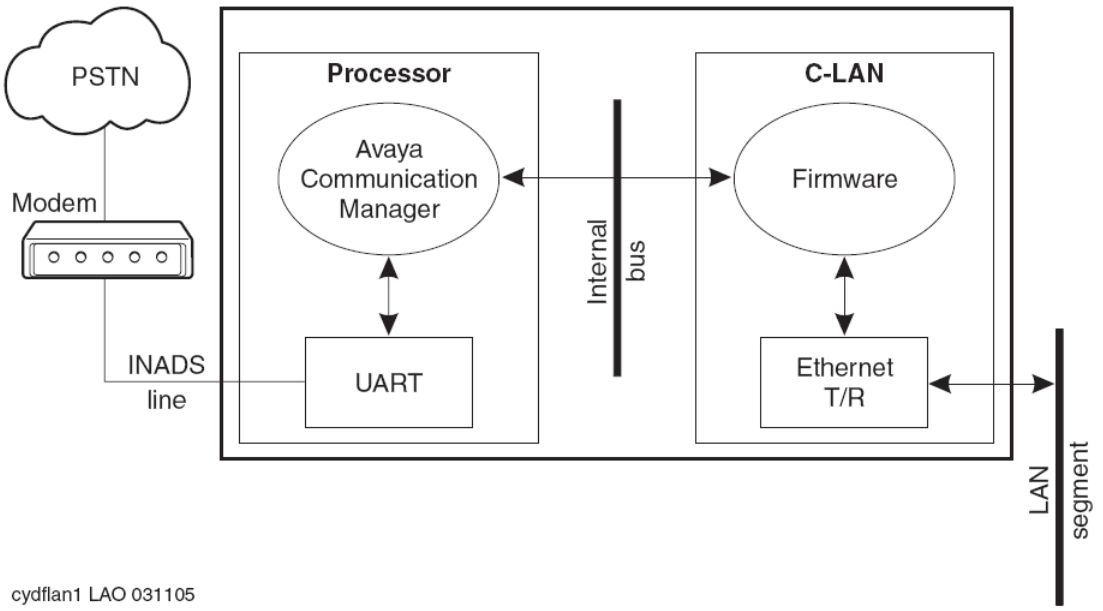
All other IP telephone models will re-register in case of server interchange.

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

Providing LAN security

Some customers are concerned that a user could access the switch using the INADS line, gain access to C-LAN, and then access to the customer’s LAN. The Avaya architecture prevents access to the customer’s LAN as depicted in Figure 1: Security-related system architecture on page 15, which shows a high-level switch schematic with a TN799 (C-LAN) circuit pack.

Figure 1: Security-related system architecture



Logins through the INADS line terminate in software; software communicates with firmware over an internal bus through a limited message set. There are two main reasons why a user cannot access a customer’s LAN through the INADS line:

- A user logging into software cannot obtain direct access to the C-LAN firmware.

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

- The C-LAN application TFTP is currently disabled and cannot be enabled by Communication Manager.

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

Connection Preservation

Communication Manager supports connection preservation and call preservation for handling SIP calls. Any SIP telephone connected through a Session Manager server with Communication Manager 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 is placed into 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 In-service/active state. When the active connection is dropped, SIP-trunk changes to Out-of-service state.
  When far-end failure is detected, the SIP signaling group is placed into the Far-end-bypass state. Stable or active calls are not dropped and the SIP-trunk changes to pending-busyout state. When the active connection is dropped, SIP-trunk changes into Out-Of-Service/ FarEnd-idle state.
- Call preservation and connection preservation when LAN connectivity is revived:
  When near-end failure is ended, SIP signaling group state changes to In-service. Stable or active calls on the SIP-trunk are kept in In-service/active state.
  When far-end failure ends, the SIP signaling group state changes to In-service, State of Stable or active calls on the SIP-trunk changes from pending-busyout to In-service/active state.

Session refresh handling

When SIP session refresh handling fails, the SIP call is set to connection preservation and a net-safety timer starts to keep the call active for 2 hours. After 2 hours the call drops, unless the user ends the call before time.

Connection Preserving Migration

The Connection Preserving Migration (CPM) feature preserves existing bearer (voice) connections while an H.248 media gateway migrates from one Communication Manager server to another because of network or server failure. However, users on connection-preserved calls cannot use such features as Hold, Conference, or Transfer, etc. In addition to preserving the audio voice paths, CPM extends the time period for recovery operations and functions during Avaya's complementary recovery strategies.

H.248 and H.323 Link Recovery

H.248 Link Recovery is an automated way in which the media gateway reacquires the H.248 link when it 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 media gateway, and the H.323 link between a media gateway and an H.323-compliant IP endpoint, provide the signaling protocol for:

- Call setup
- Call control (user actions such as Hold, Conference, or Transfer) while the call is in progress

- Call tear-down

If the link goes down, Link Recovery preserves any existing calls and attempts to re-establish the original link. If the gateway/endpoint cannot reconnect to the original server/gateway, then Link Recovery automatically attempts to connect with alternate TN799DP (C-LAN) circuit packs within the original server's configuration or to a Survivable Remote server.

Auto fallback to primary

The intent of the auto fallback to primary controller feature is to return a fragmented network, in which a number of H.248 Media Gateways are being serviced by one or more Survivable Remote servers, to the primary server in an automatic fashion. This feature is targeted towards all H.248 media gateways. By migrating the media gateways back to the primary automatically, the distributed telephony switch network can be made whole sooner without human intervention.

Survivable Remote Servers

Survivable Remote servers can act as survivable call-processing servers for remote or branch customer locations. Survivable Remote servers carry a complete set of Communication Manager features, and its license file allows it to function as a survivable call processor. If the link between the remote media gateways—G700, G450, G430, G350, or G250 and the primary controller is broken, the telephones and media gateways designated to receive backup service from the Survivable Remote servers register with the Survivable Remote server. The Survivable Remote server will provide control to those registered devices in a license error mode (see *Avaya Aura™ Communication Manager Hardware Description and Reference,* 555-245-207).

Note:

The Survivable Remote server, in contrast to the Standard Local Survivability (SLS) feature on the G250, G350, G430, and G450 Media Gateways, uses the feature known as ELS or Enhanced Local Survivability.

Survivable Core Server

The Survivable Core server feature provides survivability to port networks, H.248 Media Gateways and IP phones by allowing backup servers to be placed in various locations in the customer's network. The backup servers supply service to port networks in the case where the Avaya server fails, or connectivity to the main Communication Manager server(s) is lost. Servers for Survivable Core server can be Avaya servers, and offer full Communication Manager functionality when in survivable mode, provided sufficient connectivity exists to other Avaya components (for example, endpoints, gateways, and messaging servers).

Standard Local Survivability (SLS)

Standard Local Survivability (SLS) consists of a module built into the G250, G350, G430 and G450 Media Gateways to provide partial backup media gateway controller functionality, in the event that the connection with the primary controller is lost. This feature allows a Media Gateway, with no S8300D installed locally, to provide a degree of Communication Manager functionality when no link is available to an external controller. It is configured on a system-wide basis, or, alternatively, it can be configured on an individual Media Gateway using the CLI.

Chapter 2: Port network configurations

Communication Manager controls call processing of port networks in a large variety of ways. Control networks can be established using Ethernet connections only. Voice, fax, and TTY can be transmitted over the LAN/WAN connections. Reliability with the Duplex servers can include single control and bearer networks, duplicated control networks, duplicated control and bearer networks, or a combination of reliabilities.

IP-PNC

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

Reliability

Reliability is the ability of a Communication Manager configuration to maintain service when components such as Ethernet switches, circuit packs, or gateways within the configuration fail. The available reliability levels and their precise definitions depend on whether the port networks use IP-PNC and whether the server is simplex or duplex.

Simplex Server

A Simplex Server has several reliability options.

- Standard reliability

  For IP-PNC, a server supports a single IPSI for control in every IP-PNC PN. TN2302BP or TN2602AP circuit packs are used for the bearer network. However, TN2602AP circuit packs are implemented in load-balancing mode only.

- Duplicated bearer reliability

  For IP-PNC, an server does not support duplicated control. However, any or all IP-PNC PNs may have duplicated TN2602AP circuit packs to duplicate the bearer connections. Control signaling to a PN with duplicated TN2602AP circuit packs always occurs over a direct IPSI connection to the server. Duplicated bearer using TN2602AP circuit packs is implemented for individual PNs and does not require uniform implementation for all PNs within the configuration.

Duplex Server

A Duplex server has multiple levels of reliability.

Reliability for PNs that use IP-PNC within a single Communication Manager configuration is implemented for individual PNs and does not require uniform implementation for other IP-PNC PNs within the configuration. In addition, duplicated bearer and duplicated control can be implemented independently of each other. Duplicated control is not required for a PN to have duplicated bearer reliability.

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

- Standard duplicated servers

  A single IPSI provides control signaling between the PN and the server. Only single or load-balancing TN2302BP or TN2602AP circuit pack pairs.

- Duplicated control

  In addition to the standard duplicated servers, duplicated IPSIs for control reside in each PN. The PN 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 PN to provide duplicated bearer.

Note:
Duplicated IPSI control is recommended, but not required, for duplicated bearer for IP-PNC PNs.

- Duplicated control and bearer

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

Simplex IP-PNC (single control network)

In this configuration, the Simplex server uses IP connections to control call processing on the port networks (PNs) and to send voice between PNs over an IP network. An existing VoIP-ready IP infrastructure can be used. This solution saves customers the cost of building a separate telephony network. In this type of configuration, all PNs are connected to the server and to each other over the customer’s network. Up to 64 PNs can be configured in an IP-PNC network. Depending on the type of Ethernet switches used to connect PNs, the number of PNs, and the PN locations in the LAN and WAN, the network may require multiple Ethernet switches to support the PNs.

The following media gateway can be used in an IP-PNC network:

- G650 media gateway

  A G650 PN can consist of one to five G650 gateways in a stack connected by a TDM/LAN bus cable. One gateway, serving as control gateway in position A at the bottom of the stack, contains the following:

  - TN2312BP IPSI circuit pack

IP/TDM conversion resource: Each PN 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 PNs. These circuit packs can be inserted in any gateway in the PN. Each PN may optionally house a TN799DP C-LAN circuit pack for control of the G150 Media Gateway, the H.248 media gateways (G700, G450, G430, G350, G250), IP endpoints, adjunct systems such as messaging, and firmware downloads.

Ethernet connections. In the IP-PNC configuration, the server connects to the media gateways through a single Ethernet switch. Each PN also has a connection to the server through a local Ethernet switch. As a result, remote PNs in an IP-PNC configuration over a WAN, which normally requires routers to complete the connection, may require their own Ethernet switches, in addition to the Ethernet switch that supports the server. IP connections to the server may be administered as dedicated private LAN connections or connections over the customer LAN.

Duplicated TN2602AP circuit packs in IP-PNC PNs

For a Simplex server, any individual IP-PNC PN can contain load-balancing or duplicated TN2602AP circuit packs. However, TN2602AP circuit packs do *not* need to be implemented uniformly within the system. Thus, some PNs may have a single TN2602AP circuit pack, some PNs may have load-balancing TN2602AP circuit packs, and some PNs may have duplicated TN2602AP circuit packs. Thus, an Simplex server can have duplicated bearer connections, even though it does not support duplicated control.

Figure 2: Simplex server IP-PNC

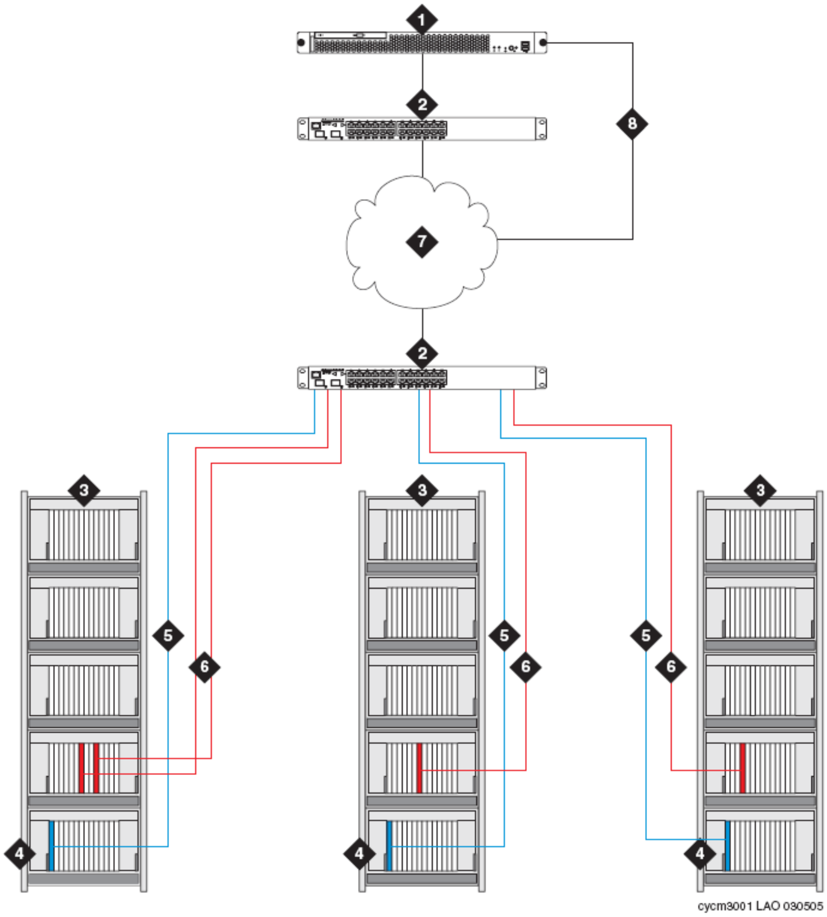


Figure notes: Simplex server IP-PNC

1. Simplex server
2. Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both the servers and the media gateways. For remote LAN/WAN connections the remote gateway(s) must have an Ethernet switches at the remote location.
3. PNs (G650 Media Gateway or stack [shown in figure]).
4. PN control gateway in the A position in the gateway stack 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 in order to provide environmental maintenance.
5. IPSI-to-server control network connection via Ethernet switch

1 of 2

Figure notes: Simplex server IP-PNC (continued)

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, PNs, and adjunct systems. These circuit packs may be inserted into a port gateway (shown in figure) or the PN control gateway.

7. Customer LAN/WAN
8. LAN connections of servers for remote administration

2 of 2

TN2602AP circuit packs for duplicated bearer

For a server, any individual IP-PNC can contain load-balancing or duplicated TN2602AP circuit packs. However, TN2602AP circuit packs do *not* need to be implemented uniformly within the system. Thus, some PNs may have no TN2602AP circuit pack, some PNs may have load-balancing TN2602AP circuit packs, and some PNs may have duplicated TN2602AP circuit packs. Thus, a server can have duplicated bearer connections, even though it does not support duplicated control.

Duplex IP-PNC (single control network)

In this configuration, the Duplex servers connect to one or more PNs over an Ethernet connection using either an interim Ethernet switch and a dedicated LAN connection or the customer's LAN. Each PN is connected to the Ethernet switch or LAN with a CAT5 cable to a TN2312AP/BP IP Server Interface (IPSI) card.

This solution saves customers the cost of building a separate telephony network. In this type of configuration, all PNs are connected to the customer's network and call control from the Duplex server is also sent over the customer's network. Up to 64 PNs can be configured in an IP-PNC network.

The following media gateways can be used in an IP-PNC network:

- G650 media gateway

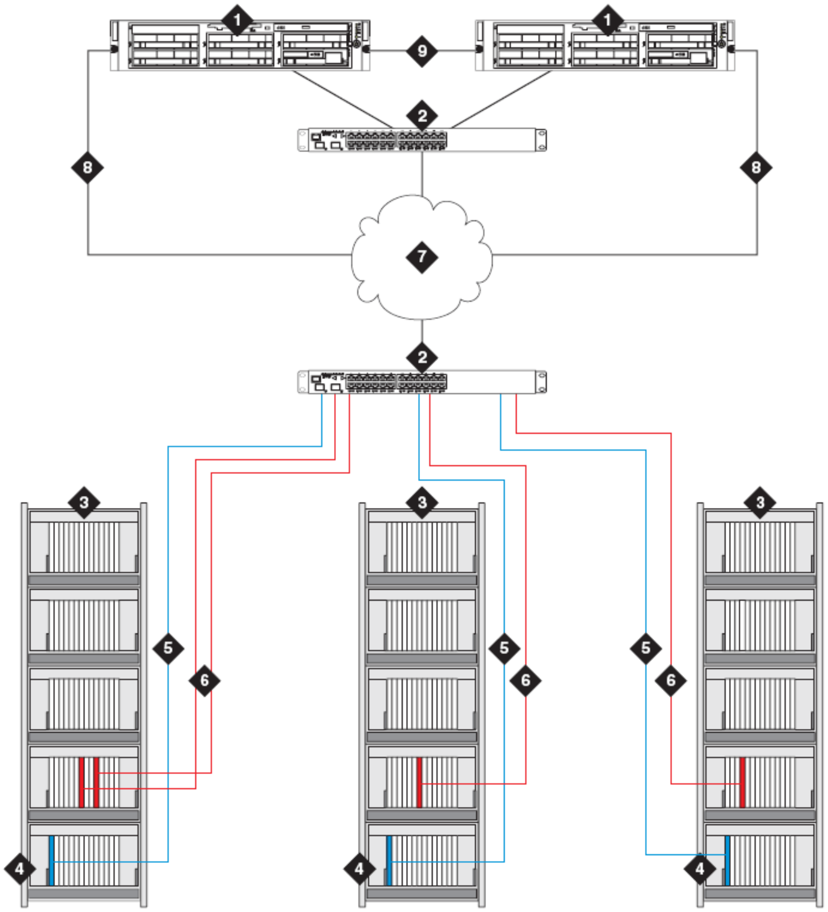
  A G650 PN can consist of one to five G650 gateways in a stack connected by a TDM/LAN bus cable. One gateway, serving as control gateway in position A at the bottom of the stack, contains the following:

  – TN2312BP IPSI circuit pack

IP/TDM conversion resource: Each PN 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 PNs. Optionally, one or more TN799DP C-LAN circuit pack can be present for control of the G150 Media Gateway, the H.248 media gateways (G700, G450, G430, G350, G250), IP endpoints, adjunct systems such as messaging, and firmware downloads. These circuit packs may be inserted in any gateway in the PN.

Ethernet connections. In the IP-PNC configuration, the Duplex server connects to the media gateways through a single Ethernet switch. Each PN also has a connection to the network or the Duplex server through a local Ethernet switch. As a result, remote PNs in an IP-PNC configuration over a WAN, which normally requires routers to complete the connection, may require their own Ethernet switches in addition to the Ethernet switch that supports the Duplex server. IP connections to the Duplex server may be administered as dedicated private LAN connections or connections over the customer LAN.

Figure 3: Duplex IP-PNC single control network



cycm3003 LAO 030505

Figure notes: Duplex IP-PNC single control network

1. Duplex Server

2. Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both the servers and the media gateways. For remote LAN/WAN connections, the remote gateway(s) must have an Ethernet switches at the remote location.

3. PNs (G650 Media Gateway or stack [shown in figure]).

4. PN 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 in order 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, PNs, and adjunct systems. These circuit packs may be inserted into a port gateway (shown in figure) or the PN control gateway.

1 of 2

Figure notes: Duplex IP-PNC single control network (continued)

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 board or (for the Duplex Server) through software duplication.

2 of 2

Duplex IP-PNC (duplicated control network)

The Duplex server IP-PNC high reliability configuration is the same as the standard reliability configuration, except for the following differences:

- There are duplicated Ethernet switches, with each server connected to each Ethernet switch
- Each PN has duplicated TN2312AP/BP IPSI circuit packs. One IPSI circuit pack in each PN is connected through one Ethernet switch and the other IPSI circuit pack is connected through the other Ethernet switch

Figure 4: Duplex IP-PNC duplicated control network

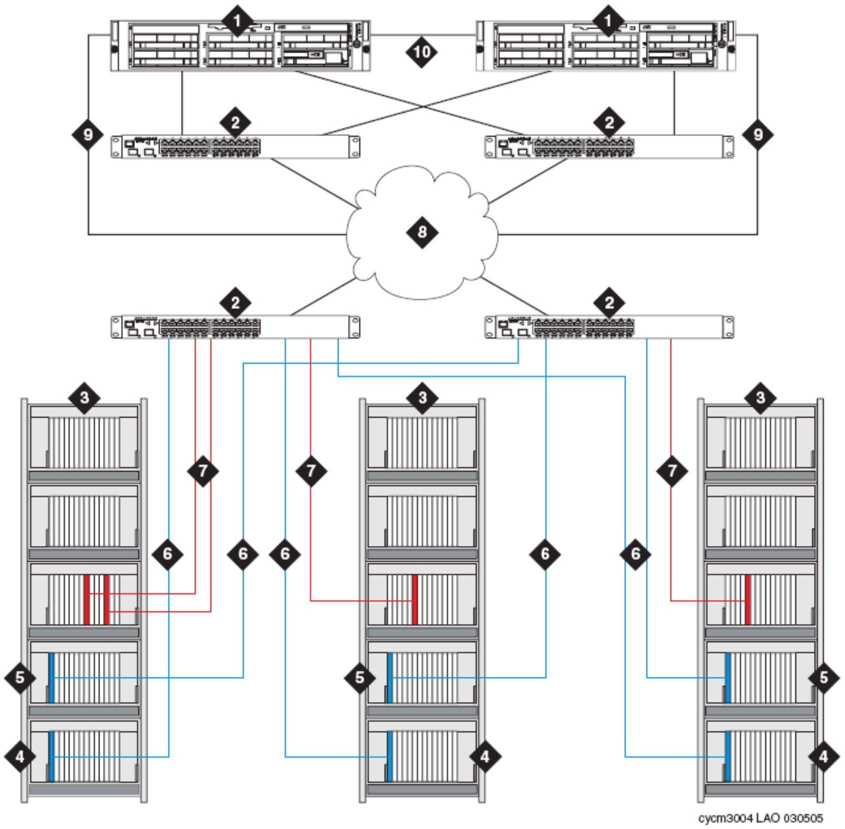


Figure notes: Duplex IP-PNC duplicated control network

1. Duplex Server
2. Ethernet Switch. For local LAN connections, the same pair of Ethernet switches can connect both the servers and the media gateways. For remote LAN/WAN connections, the remote gateway(s) must have a pair of Ethernet switches at the remote location.
3. PNs (G650 Media Gateway or stack [shown in figure]).
4. PN 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 in order 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, PNs, and adjunct systems. These circuit packs may be inserted into a port carrier (shown in figure), the PN control carrier, or the duplicated control carrier.

1 of 2

Figure notes: Duplex IP-PNC duplicated control network (continued)

8. Customer LAN

9. LAN connections of servers for remote administration

10. 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 board or (for the Duplex Server) through software duplication.

2 of 2

Duplex IP-PNC (duplicated control and duplicated bearer network)

The Duplex Server IP-PNC critical reliability configuration (duplicated control and duplicated bearer network) is the same as the high reliability configuration, except for the following differences:

- Each PN has duplicated TN2602AP IP Media Resource 320 circuit packs. One TN2602 circuit pack in each PN is connected through one Ethernet switch and the other TN2602 circuit pack is connected through the other Ethernet switch.
- A TN771DP Maintenance Test circuit pack must also be installed in each PN that has duplicated control and bearer network connections.

Figure 5: Duplex IP-PNC duplicated control and duplicated bearer network

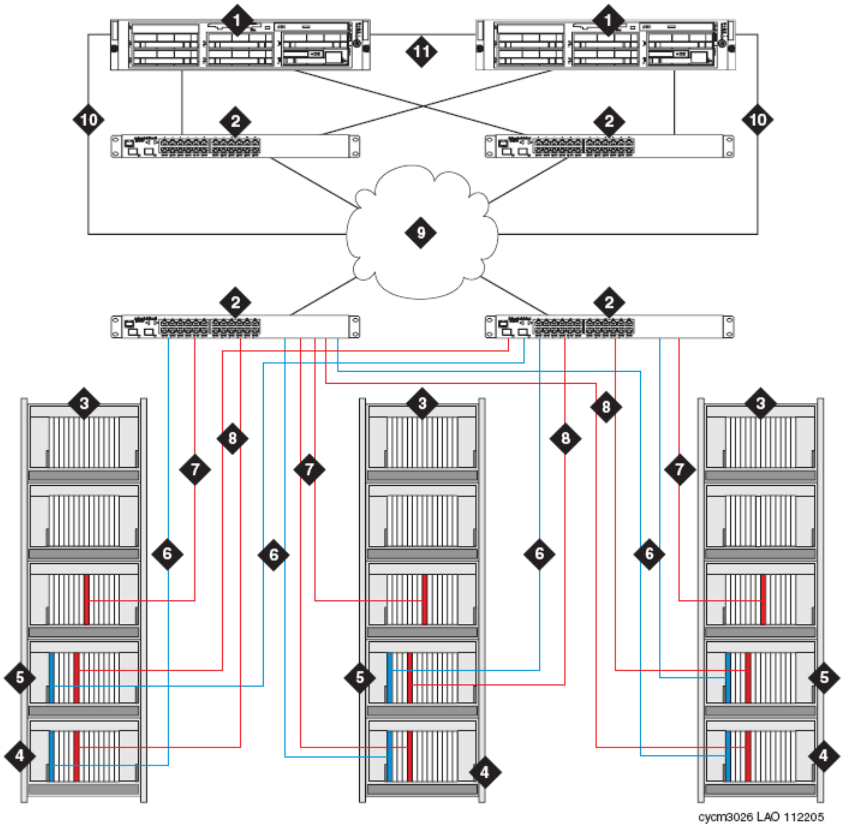


Figure notes: Duplex IP-PNC duplicated control and duplicated bearer network

1. Duplex Server

2. Ethernet Switch. For local LAN connections, the same pair of Ethernet switches can connect both the servers and the media gateways. For remote LAN/WAN connections, the remote gateway(s) must have a pair of Ethernet switches at the remote location.

3. PNs (G650 Media Gateway or stack [shown in figure]).

4. PN 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 in order to provide environmental maintenance.
   - A TN2602AP IP Media Resource 320 for PN bearer connections over the LAN

     NOTE: The TN2602AP circuit pack may be placed in any gateway in the PN. However, the pair of TN2602 circuit packs should be separated between two different gateways whenever 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 PN bearer connections over the LAN

     NOTE: The TN2602AP circuit pack may be placed in any gateway in the PN. However, the pair of TN2602 circuit packs should be separated between two different gateways whenever possible.

1 of 2

Figure notes: Duplex IP-PNC duplicated control and duplicated bearer network

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, PNs, and adjunct systems. These circuit packs may be inserted into a port carrier (shown in figure), the PN control carrier, or the duplicated control carrier.
8. LAN connections of TN2602AP IP Media Resource 320 circuit packs for IP-TDM voice processing
9. Customer LAN
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 board or (for the Duplex Server) through software duplication.

2 of 2

Example of IP-PNC PNs with different reliability levels

Figure 6 illustrates a Duplex Server configuration that combines duplicated control/duplicated bearer network, duplicated control-only network, and single control network reliability configurations in an IP-PNC network. The PN with a single control network is labeled as item 11. Other PNs, items 3, have duplicated control networks.

Figure 6: IP-PNC PNs with single control network, duplicated control networks, and duplicated control/bearer network example

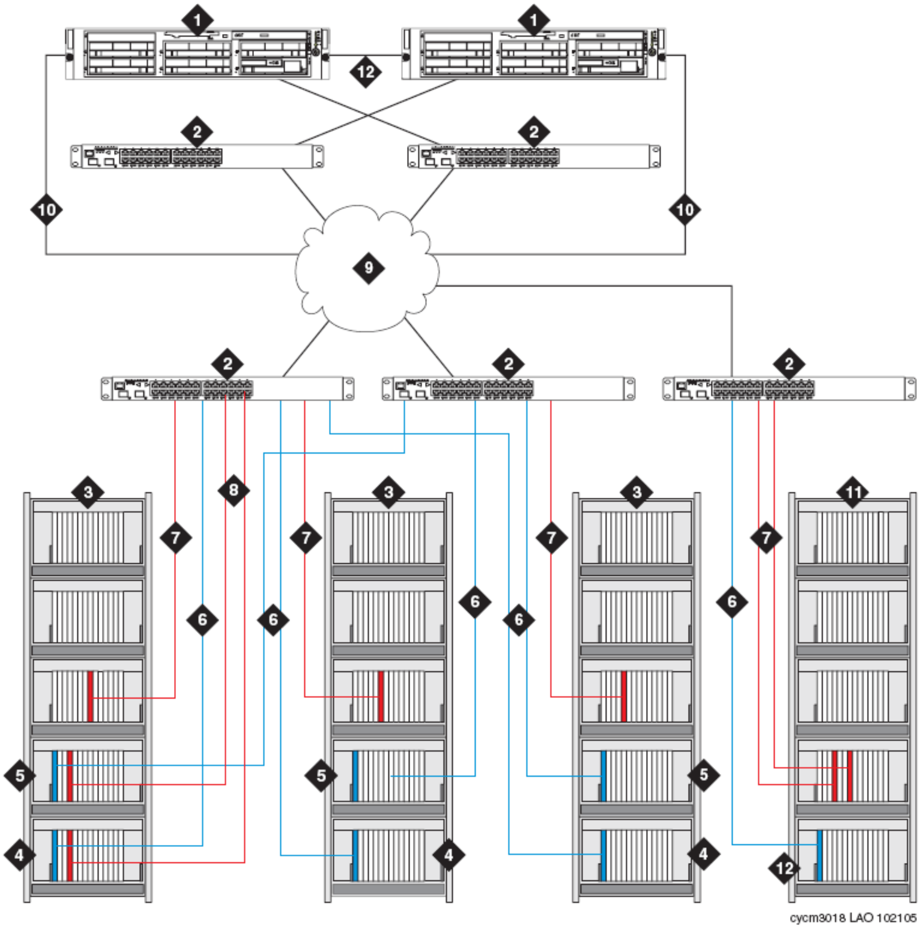


Figure notes: IP-PNC PNs with single, duplicated control networks, and duplicated control/bearer network)

1. Duplex server

2. Ethernet Switch. For local LAN connections, the same pair of Ethernet switches may connect both the servers and the media gateways. For remote LAN/WAN connections, the remote gateway(s) must have a pair of Ethernet switches at the remote location.

3. IP-PNC PNs (G650 Media Gateway or stack [shown in figure]).

4. Control gateway for PN 3, in the A position in the gateway stack. The control gateway contains:
   - A TN2312AP/BP IPSI circuit pack for IP connection to server.

5. Duplicated PN control gateway for PN3, in the B position in the gateway stack. The control gateway contains:
   - A TN2312AP/BP IPSI circuit pack for IP connection to control network.

6. IPSI-to-server control network connection via Ethernet switch

1 of 2

Figure notes: IP-PNC PNs with single, duplicated control networks, and duplicated control/bearer network) (continued)

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 may be inserted into a port carrier (shown in figure), the PN control carrier, or the duplicated control carrier.

8. Customer LAN

9. LAN connections of servers for remote administration

10. 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 software duplication.

11. IP-PNC PN (G650 Media Gateway or stack [shown in figure]).

12. PN control gateway, in the A position in the gateway stack, for PN 11. The control gateway contains:

- A TN2312AP/BP IPSI circuit pack for IP connection to server.

2 of 2

Chapter 3: Control Networks

Control Networks carry the call signaling data between call servers and the port networks. A control network is an Ethernet link between an Ethernet port on the Simplex or Duplex server and an Ethernet port on an IPSI circuit pack in a port network, possibly with intermediate switches.

Before upgrading Communication Manager from some earlier version to Release 6.0, you must remove private control networks and place all IPSI on the network that connects the Communication Manager server to the corporate LAN. Communication Manager 6.0 allows customers to use their network infrastructure without dedicated Control Networks and no longer impose restrictions such as mandating the use of CNA or CNB.

The following sections illustrate scenarios involved in consolidating your Control Networks:

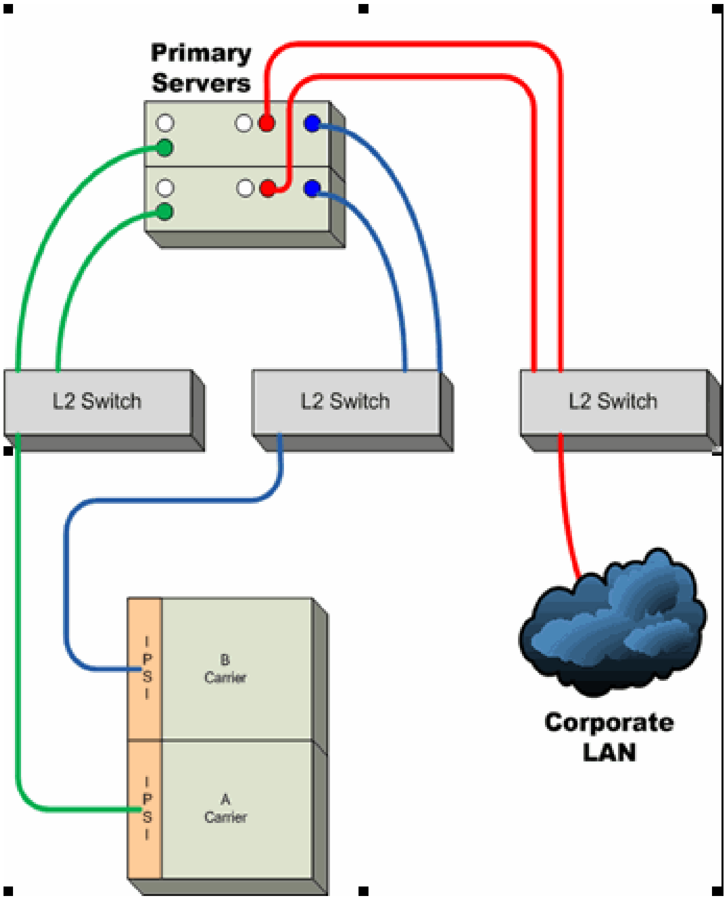
- Connect duplicated Control Networks through Layer 2 switches
- Move duplicate Control Networks from multiple Layer 3 to a single Layer 3
- Implement NIC Bonding at the main server.

For more information about the procedure to consolidate your control network, see *Upgrading to Avaya Aura*^{TM} *Communication Manager Release 6.0 (03-603560).*

Connect duplicated Control Networks through Layer 2 switches

Figure 7 illustrates the method to connect a duplicated control network A and a control network B, on a private subnet, through independent layer 2 switches.

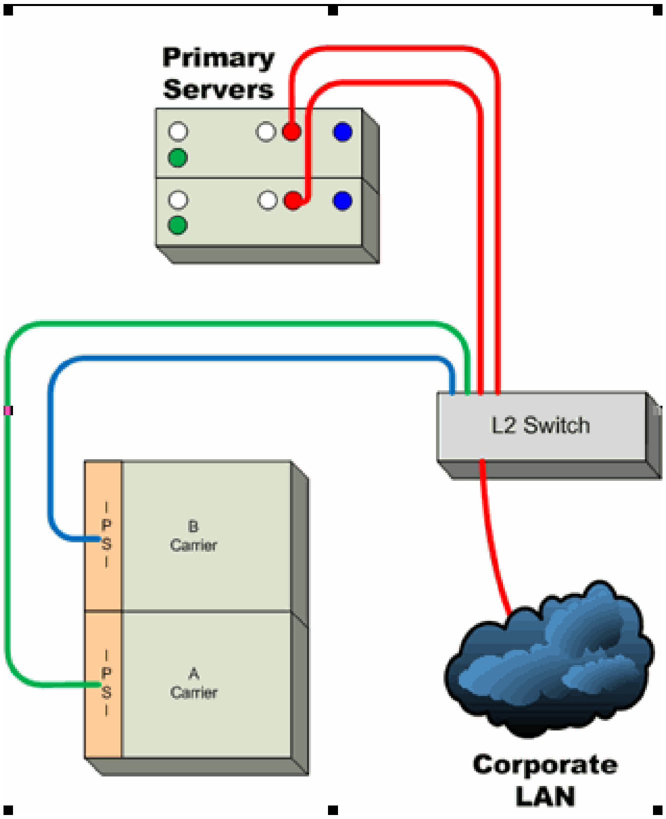
Figure 7: Duplicate control networks connected through Layer 2 switches



Move duplicate Control Networks from multiple Layer 3 to a single Layer 3

Figure 8 illustrates the method to move control networks from multiple layer 3 managed private subnets to a single layer 3 corporate LAN.

Figure 8: Move duplicate control networks from multiple layer to a single layer

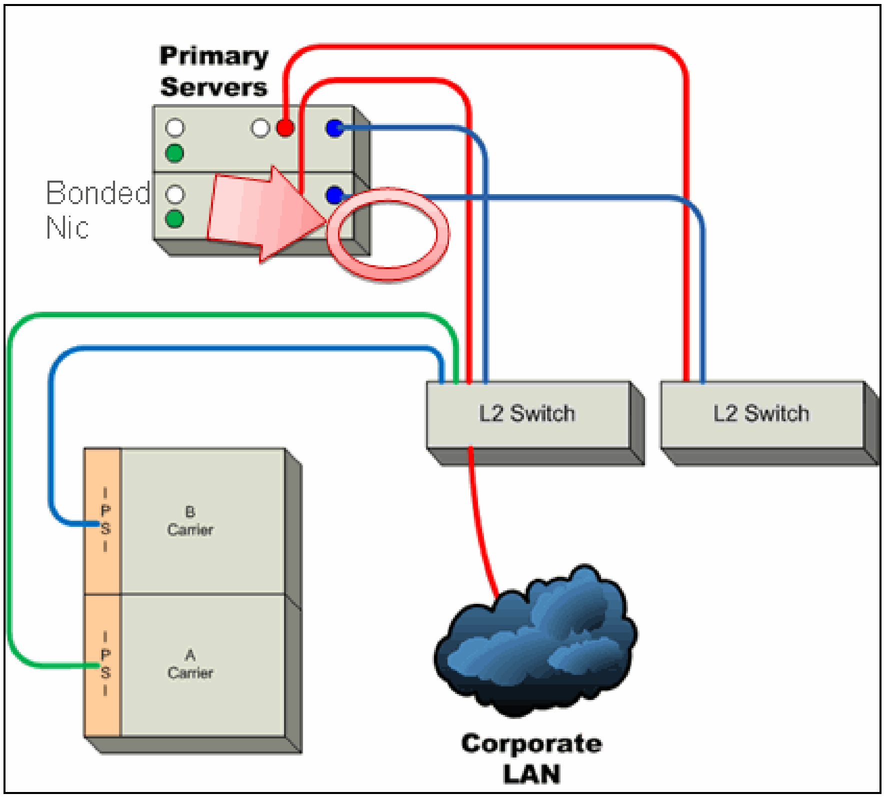


Implement NIC Bonding at the main server

NIC bonding uses multiple network cables or ports in parallel to increase the link speed beyond the limits of any one single cable or port and to increase the redundancy for higher availabilty. Two NICs are bonded together to appear as if they are the same physical device, that is, they both have the same MAC address. NIC bonding provides backup if the promary Security Module interface fails or its port is switched off.

Instead of providing the resiliency at your IPSI's, you can now provide the same functionality at the main server through the implementation of NIC bonding. In such a case, each server will have its primary Eth0 port, as indicated in the Figure 9 in red, separated out to a different layer 2 switch.

Figure 9: Bonded NIC



Before attempting NIC bonding it is highly recommended that you verify the integrity and functionality of each NIC on its own. The cable itself or either of the ports, the cable is plugged into, can fail.

When NIC bonding is activated, the Security Module uses Eth2 as the primary interface and the Eth3 as the secondary backup interface. A logical interface called bond0 is created to connect the two interfaces and has the IP address of the Security Module. Alarms are generated when one of the interfaces (Eth2 or Eth3) is down. When both the interfaces are down, an alarm is generated indicating that the bond0 interface is down.

For more information about NIC bonding, see *Administering Avaya Aura^{TM} Session Manager (03-603324)*.

Chapter 4: Administering converged networks

This section provides information for administering converged network components.

Note:

> The SAT screens shown in this guide are examples only. They are not guaranteed to match real CM 6.0 SAT screens.

About 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. Avaya's VoIP technology provides a cost-ive and flexible way of building enterprise communications systems through a converged network.

Some of the flexible elements of a converged network include:

- Separation of call control and switching functions. See *Separation of Bearer and Signaling section in Avaya Aura* ^{TM} *Commumnication Manager Feature Description and Implementation,* 555-245-205.
- 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 the network bandwidth, or the total information throughput that the network can deliver. Data traffic tends to require 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 ively, but when digitized voice signals are added to the mix, networks must be managed differently to ensure constant, real-time transmission needed by voice.

Providing a network assessment

Even if your network appears to perform acceptably, 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 appear to be stable and perform at acceptable levels, but have performance and stability issues that create problems for Avaya VoIP Solutions. While a customer network may appear to be ready to support full-duplex VoIP applications, Avaya cannot assure performance and quality without a network assessment.

The network assessment services for Avaya VoIP consist of 2 phases:

- Basic Network Assessment — is a high-level LAN/WAN infrastructure evaluation that determines the suitability of an existing network for VoIP.
- Detailed Network Assessment — is typically the second phase in the Network Assessment for IP Telephony solutions.

  The detailed network assessment takes information gathered in the basic network assessment, performs problem diagnosis, and provides functional requirements for the network to implement Avaya VoIP.

For more information, see

- "Network assessment offer" in *Avaya Application Solutions: IP Telephony Deployment Guide*, 555-245-600.
- Avaya Professional Services - The Avaya Professional Services support a portfolio of consulting and engineering offers to help plan and design voice and data networks.

Setting up VoIP hardware

This section contains descriptions and administration information for the following circuit packs and media modules:

- About Universal DS1 circuit packs and MM710 T1/E1Media Module
- About the TN799DP Control LAN
- About the TN2302AP IP Media Processor
- About the TN2602AP IP Media Resource 320
- About the TN2312BP IP Server Interface
- About the MM760 VoIP Media Module
- About the Processor Ethernet

About 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 with the addition of echo cancellation circuitry, which 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 intended for users who encounter echo over circuits connected to the Direct Distance Dialing (DDD) network. Echo is most likely to be noticeable when Communication Manager is configured for 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 their circuits.

Echo cancellation is a software right-to-use feature that supports voice channels, and is not intended for data. When a data call is received, these circuit packs detect a modem tone and turn off echo cancellation for the duration of the data call.

Working with echo cancellation

You can determine whether echo cancellation is enabled for TN464HP/TN2464CP circuit packs and MM710 T1/E1 Media Modules by displaying the **system-parameters customer-options** screen.

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

2. Find and review the following fields.

   The fields may appear on different pages of the screen.

Field	Conditions/Comments
Maximum Number of DS1 Boards with Echo Cancellation	Specifies the number of DS1 boards that have echo cancellation turned on.
DS1 Echo Cancellation	If **y**, echo cancellation is enabled.

3. Exit the screen.

Administering echo cancellation on the DS1 circuit pack or MM710 media module

Note:

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

The **DS1 Circuit Pack** screen for the TN464HP/TN2464CP circuit packs and MM710 media module has fields to support echo cancellation: **Echo Cancellation**, **EC Direction**, and **EC Configuration**. The **Echo Cancellation** field appears when the Echo Cancellation feature is activated on the **System-Parameters Customer Options** screen. The **EC Direction** and **EC Configuration** fields appear when the **DS1 Echo Cancellation** field is enabled.

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

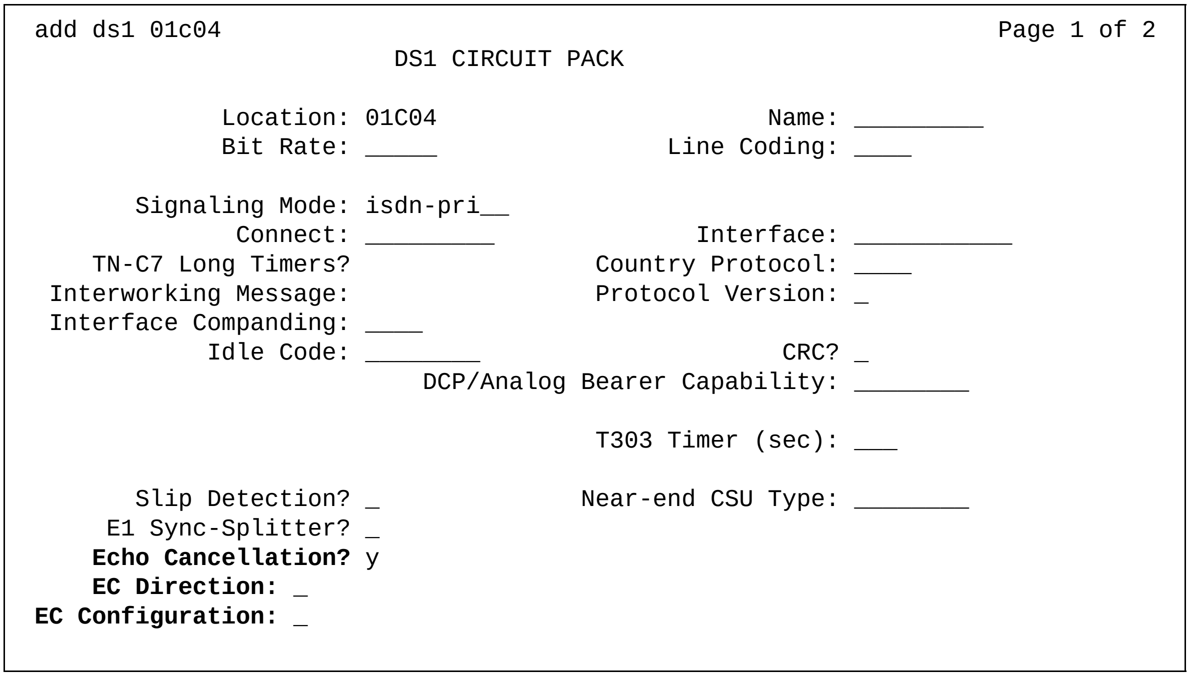
  This information is stored in firmware on the UDS1 circuit pack.

To administer the DS1 circuit pack and MM710 media module

1. Type **add ds1 *<port>*** and press **Enter** to open the **DS1 Circuit Pack** screen,

   where ***<port>*** is the location of the DS1 circuit pack, or the MM710 media module.

DS1 Circuit Pack screen



```
add ds1 01c04                                                           Page 1 of 2
                         DS1 CIRCUIT PACK

             Location: 01C04                         Name: _________
             Bit Rate: _____                  Line Coding: ____

       Signaling Mode: isdn-pri__
              Connect: _________                Interface: ___________
    TN-C7 Long Timers?                   Country Protocol: ____
  Interworking Message:                  Protocol Version: _
  Interface Companding: ____
            Idle Code: ________                      CRC? _
                           DCP/Analog Bearer Capability: ________

                                         T303 Timer (sec): ___

       Slip Detection? _                Near-end CSU Type: ________
     E1 Sync-Splitter? _
    Echo Cancellation? y
    EC Direction: _
EC Configuration: _
```

2. On the **DS1 Circuit Pack** screen, complete the following fields:

Field	Conditions/Comments
Echo Cancellation	Enter **y** to enable echo cancellation on the Universal DS-1 circuit pack.
EC Direction	Indicates the direction of the echo that is being cancelled. Enter **inward** or **outward**. ● The **inward** setting cancels echo energy coming back into the switch — energy from an outgoing call is reflected from an external reflection point (party "inside" the switch hears the echo). ● The **outward** setting cancels echo energy going outside the switch — energy from an incoming call is reflected from an internal reflection point (party "outside" the switch hears the echo).

Field	Conditions/Comments
EC Configuration	Indicates the set of echo cancellation defaults to administer. Appears when the Echo Cancellation field is set to **y**. Enter digits between **1-15**. ● Enter **1** or **5-15** to provide most rapid adaptation in detecting and correcting echo at the beginning of a call, regardless of the loudness of the talker's voice. For very loud talkers and severe echo, the far-end talker's speech is heard as clipped when both parties talk at the same time. ● Enter **2** for slightly slower adaptation to echo, use if speech is often clipped when both parties talk at the same time. ● Enter **3** for slightly slower adaptation to echo, may result in a 2 or 3 second fade on strong echo for quiet talkers. Completely removes speech clipping. ● Enter **4** in cases of extreme echo, excessive clipping or breakup of speech. May result in slight echo or background noise. **Note:** For the MM710, the values **1** and **4** are reversed. That is, **1** for the MM710 is the same as **4** for the TN464HP/ TN2464CP, and **4** for the MM710 is the same as **1** for the TN464HP/ TN2464CP

Administering echo cancellation on trunks

Note:

> Changes to echo cancellation settings on the Trunk Features screen do not take until after a port or trunk group is busied-out/released, or the SAT command **`test trunk group`** is performed, or periodic maintenance is run.

Echo cancellation is turned on or off on a per trunk-group basis using the **`change trunk-group`** command. If the trunk group field, **DS1 Echo Cancellation** is y, echo cancellation is applied to every TN464HP/TN2464CP trunk member in that trunk group. The echo cancellation parameters used for a given trunk member are determined by the **EC**

Configuration number administered on the **DS1 Circuit Pack** screen for that specific trunk's board.

Echo cancellation applies to voice channels and supports echo cancellation on the following trunk group types:

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

Administration of echo cancellation on a trunk group is done on the **TRUNK FEATURES** screen.

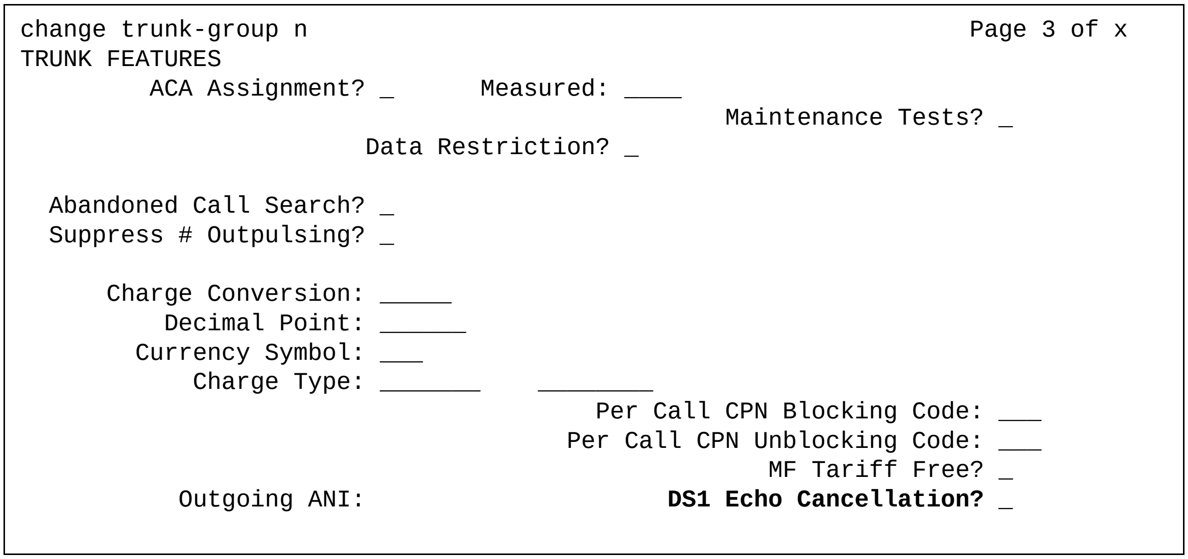
To administer a trunk group for echo cancellation

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

   where ***n*** is the trunk group number.

2. Go to the Trunk Features page. Note: the fields displayed depend on the trunk group type.

Trunk Features screen



```
change trunk-group n                                              Page 3 of x
TRUNK FEATURES
         ACA Assignment? _      Measured: ____
                                                 Maintenance Tests? _
                        Data Restriction? _

  Abandoned Call Search? _
  Suppress # Outpulsing? _

      Charge Conversion: _____
          Decimal Point: ______
        Currency Symbol: ___
            Charge Type: _______    ________
                                        Per Call CPN Blocking Code: ___
                                      Per Call CPN Unblocking Code: ___
                                                    MF Tariff Free? _
           Outgoing ANI:                             DS1 Echo Cancellation? _
```

3. Move to the following field

Field	Conditions/Comments
DS1 Echo Cancellation	Enter **y** to enable echo cancellation on a per trunk group basis.

4. Save the changes.

About the 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 or Processor Ethernet, see TN799DP control LAN (C-LAN) interface on page 12 in the Network quality management section of the Networking Overview chapter.

The C-LAN handles the data-link signaling information in one of two configurations: Ethernet, or point-to-point (PPP). 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, the C-LAN passes the signaling information over a separate TCP/IP network, usually by means of a hub or Ethernet switch.

  Avaya recommends 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, the C-LAN passes the data-link signaling to the DS1 for inclusion 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. The appropriate DS1 circuit packs must be installed, if they 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 MAC address of the C-LAN circuit pack. 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

The 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

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, be sure you understand the requirements of your LAN. For information about LAN requirements for VoIP, see *Avaya IP Voice Quality Network Requirements* at Avaya support site https://support.avaya.com

The following steps describe installation for the TN799DP C-LAN.

1. Determine the carrier/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 specified in step 1.

   Note:

   You do not need to power down the cabinet to install a C-LAN circuit pack.

Installing C-LAN cables to a hub or ethernet switch

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

Assigning IP node names and IP addresses

Communication Manager uses node names to reference IP addresses through out the system.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.

You should assign the node names and IP addresses logically and consistently across the entire network. These names and addresses should be assigned in the planning stages of the network and should be available from the customer system administrator or from an Avaya representative.

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

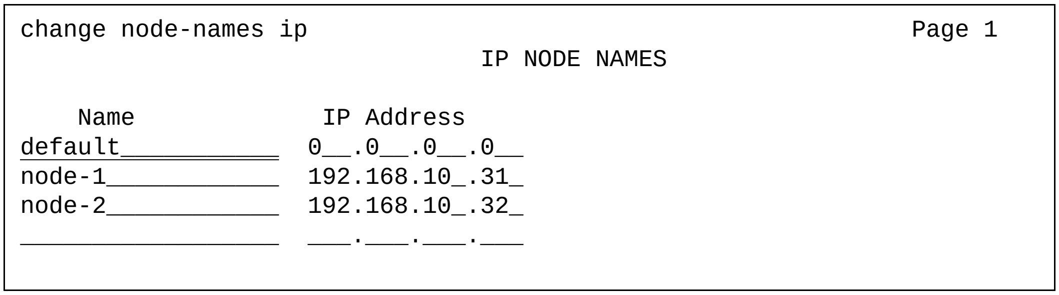
- Communication Manager Messaging Address

Enter the IP address on the **IP Node Names** screen. Enter data for all the 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.

To assign IP node names:

1. Type **`change node-names ip`** and press **Enter** to open the **IP Node Names** screen.



```
change node-names ip                                          Page 1
                                IP NODE NAMES

    Name             IP Address
default___________  0__.0__.0__.0__
node-1____________  192.168.10_.31_
node-2____________  192.168.10_.32_
__________________  ___.___.___.___
```

2. Enter values as follows.

Field	Conditions/Comments
Name	Enter unique node names for ● Each C-LAN Ethernet port on the network ● Each IP Media Processor ● Each Remote office ● Other IP gateways, hops, etc. The default node name and IP address is used to set up a default gateway, if desired. 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.
IP Address	Enter unique IP addresses of the nodes named in the previous field.

3. Submit the screen.

Defining a LAN default gateway

On LANs that connect to other networks or subnetworks, Avaya recommends that you define a default gateway. The default gateway node is a routing device that is connected to different (sub)networks. Any packets addressed to a different (sub)network, 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 (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. It acts as a variable that takes on unknown addresses as values. When the “default” IP route is set up, any address not known by the C-LAN is substituted for the default address in the default IP route, which uses the router as the default gateway.

Setting up 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. This increases system performance and reliability.

If registration with the original C-LAN circuit pack IP address is successful, the software sends back the IP addresses of all the C-LAN circuit packs in the same network region as the IP endpoint. If the network connection to one C-LAN circuit pack fails, the IP endpoint re-registers with a different C-LAN. If the system uses network regions based on 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 also be used if 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 or in the script downloaded from the Trivial File Transfer Protocol (TFTP) server. If the phone cannot contact the first gatekeeper address, it uses an alternate address. If the extension and password is rejected by the first gatekeeper, the IP Telephone contacts the next gatekeeper. The number of gatekeeper addresses the phone accepts depends on the length of the addresses administered on the DHCP server.

Note:

> A single Alternate Gatekeeper list is typically used in configurations with multiple servers. In this case, the DHCP server sends the same Alternate Gatekeeper list to all IP endpoints, but a given IP endpoint may not be able to register with some of the gatekeepers in the list and a registration attempt to those gatekeepers will be rejected. For more information on the Alternate Gatekeeper Lists(AGL), see *Avaya Aura ^{TM} Communication Manager Screen Reference, 03-602878*.

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

Note:

DHCP servers send a list of alternate gatekeeper and C-LAN addresses to the IP Telephone endpoint. It is possible for a hacker to issue a false request and thereby obtain IP addresses from the DHCP server. However, the alternate gatekeeper IP addresses will only be sent to an endpoint that successfully registers.

About the TN2302AP IP Media Processor

Use the TN2302AP IP Media Processor to transmit voice and FAX data (non-DCS signaling) over IP connections, and 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, and its design improves voice quality through its dynamic jitter buffers.

The TN2302AP IP Media Processor additionally performs the functions:

- Echo cancellation
- Silence suppression

- DTMF detection
- Conferencing

It supports the following codecs, FAX detection for them, and conversion between them:

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

Improving the TN2302AP transmission interface

The TN2302AP IP Media Processor provides improved voice quality through its dynamic jitter buffers. The TN2302AP's digital signal processors (DSPs), by default, insert 5.0 dB of loss in the signal from the IP endpoints, and insert 5.0 dB of gain in the signal to the IP endpoints. System administrators can administer loss/gain, based on country code on the **terminal-parameters** screen.

Supporting 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 simple change of addressing. This reduces delay and leaves DSP resources available.

Testing 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.

About the TN2602AP IP Media Resource 320

The TN2602AP IP Media Resource 320 provides high-capacity voice over Internet protocol (VoIP) audio access to the switch for local stations and outside trunks. 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

Only two TN2602AP circuit packs are allowed per port network.

Note:

The TN2602AP IP Media Resource 320 is not supported in CMC1 and G600 Media Gateways.

Load balancing

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

Note:

When two TN2602AP circuit packs, each with 320 voice channels, are used for load balancing within a port network, the total number of voice channels available is 484, because 484 is the maximum number of time slots available for a port network.

Bearer duplication

Two TN2602AP circuit packs can be installed in a single port network (PN) for duplication of the bearer network. In this configuration, one TN2602AP is an active IP media processor and one is a standby IP media processor. If the active media processor, or connections to it, fail, active connections failover to the standby media processor and remain active. This duplication prevents active calls in progress from being dropped in case of failure. The interchange between duplicated circuit packs affects only the PN 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 PN share a virtual IP and virtual MAC address. These virtual addresses are owned by the currently-active TN2602. In addition to the virtual IP address, each TN2602 has a "real" IP address. All bearer packets sent to a PN that contains duplicated TN2602AP circuit packs, regardless of whether the packets originate from TN2602s in other PNs or from IP phones or gateways, are sent to the virtual IP address of the TN2602 pair in that PN. Whichever TN2602AP circuit pack is active is the recipient of those packets.

When failover to the standby TN2602 occurs, a negotiation between TN2602s to determine which TN2602 is active and which is standby takes place. 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 to ensure that the LAN infrastructure is updated appropriately with the location of the active TN2602. Other devices within the LAN will update their old mapping in ARP cache with this new mapping.

Requirements for bearer duplication

The Communication Manager license file must have entries for each circuit pack, with the entries having 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. In addition, the Ethernet switch or switches that the circuit packs connect to must also be in the same subnet. This shared subnet allows the Ethernet switches to use signals from the TN2602AP firmware to identify the MAC address of the active circuit pack. This identification process provides a consistent virtual interface for calls.

Combining duplication and load balancing

A single port network can have up to two TN2602AP circuit packs only. As result, the port network can have either two duplicated TN2602AP circuit packs or two load balancing TN2602AP circuit packs, but not both a duplicated pair and a load-balancing pair. 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 single or no TN2602AP circuit packs.

Note:

If a pair of TN2602AP circuit packs previously used for load balancing are re-administered to be used for bearer duplication, only the voice channels of whichever circuit pack is active can be used. For example, If you have two TN2602 AP circuit packs in a load balancing configuration, each with 80 voice channels, and you re-administer the circuit packs to be in bearer duplication mode, you will have 80 (not 160) channels available. If you have two TN2602 AP circuit packs in a load balancing configuration, each with 320 voice channels, and you re-administer the circuit packs to be in bearer duplication mode, you will have 320 (rather than 484) channels available.

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 (320 ms)
- 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 pass-through mode
- Fax, V.32 modem, and TTY calls using 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 to itself. However, this capability is activated by and available for authorized services personnel only.

As with the TN2302AP IP Media Processor, firmware upgrades of the TN2602AP circuit pack, are not call preserving. 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 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 also requires an input/output adapter that provides for one RS-232 serial port and two 10/100 Mbs Ethernet ports for LAN connections (though only the first Ethernet port is used). This Ethernet connection is made at the back of the IP Media Resource 320 slot.

Note:

The About the TN2302AP IP Media Processor on page 48 can also use this I/O adapter.

About the TN2312BP IP Server Interface

In configurations with the Duplex server controlling media gateways, the bearer paths and the control paths are separate. Control information for port networks (PNs) travels over a LAN through the Ethernet switch. The control information terminates on the Duplex server at one end and on a TN2312BP IP Server Interface (IPSI) on the other end. Each IPSI may control up to five port networks by tunneling control messages over the Center-Stage to PNs that do not have IPSIs.

Note:

IPSIs cannot be placed in a PN that has a Stratum-3 clock interface. Also, IPSIs cannot be placed in a remote PN that is using a DS1 converter.

In configurations that use a dedicated LAN for the control path, all IPSI must be statically addressed. IPSIs on Dedicated control networks must be configured to be connected to the corporate LAN.

Consult the Avaya S8300D, Simplex and Duplex server Library CD (555-233-825) for information on installing and upgrading Duplex servers and IPSI configurations.

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, Media Gateways and Servers*, 300431.

Detailed description

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

- Set the values of QoS parameter fields (**DiffServ** and **802.1p**) on the System Parameters IP Server Interface screen. Default value for **DiffServ** is **46** and **802.1p** is **6**.
- Download QoS parameters to all IPSI boards. By default, **`add ipserver-interface`** or **`change ipserver-interface`** command pre-populates the QoS parameters if any IPSI boards are added.
- Set the values of Ethernet interface fields (**Auto**, **Speed**, or **Duplex**) on the IP Server Interface screen. **Speed** and **Duplex** fields appear on the IP Server Interface screen, if **Auto** field is set to **n**.

- Changes to IPSI IP addresses (**IP Address**, **Subnet Mask, Gateway** address) on the IP Server Interface screen.

  Note:

  The initial IPSI IP address must be set manually by locally logging on to each IPSI board through a telnet or an ssh connection).

Firmware requirements

The IPSI and the Communication Manager system use a capabilities exchange message to determine if an IPSI/SIPI board is capable of supporting the IPSI administration feature. IPSI firmware version 46 or greater and SIPI firmware version 16 or greater are required to support this capabilities exchange upon the port network coming into service.

IP Server Interface parameters

The IPSI sends QoS parameters, Ethernet settings, and IP address information to Communication Manager as specified in the Table 2. The exchange of information is shared on socket creation.

⚠ **WARNING:**

If the Ethernet interface settings (**Auto**, **Speed**, and **Duplex**) or the IPSI IP address settings (**IP Address**, **Subnet Mask**, and **Gateway** address) do not match with the network entity that the IPSI is communicating with, network communication may 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**. Enable VLAN 802.1q priority tagging On the IP Server Interface screen Use System Level Parameter Values **802.1p** value **DiffServ** value		No
Ethernet interface settings: On the IP Server Interface screen Auto Speed Duplex	You need to reset the IPSI board for **Auto**, **Speed**, and **Duplex** values to take .	Yes
IP Address information: On the IP Server Interface screen IPSI **IP Address** Subnet Mask **Gateway** address	You need to reset the IPSI board for **IP Address**, **Subnet Mask**, and **Gateway** address values to take .	Yes

Communication Manager alarm on settings mismatch

Communication Manager compares its administered values on the 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** value
- **DiffServ** value
- Ethernet **Auto** value
- Ethernet **Speed** value
- Ethernet **Duplex** value

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

Note:

Discrepancy between the SAT administration and the IPSI board values can happen if you have changed any of the IPSI board values using the CLI interface.

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 interface.

Default settings of IPSI QoS parameters

In the IPSI administration feature, QoS settings are standardized to communicate between the IPSI and Communication Manager. You can administer QoS parameters information on the Change IP Server Interface screen. The QoS default settings are shown in the following Table 3.

Table 3: QoS default settings

Description	**Defaults**	**How to administer**
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
	802.1p = **6**	**802.1p** field on **change ipserver-interface** SAT screen. Or, IPSI CLI interface
	802.1p/Q enabled = **no**	IPSI CLI interface

Backward compatibility

The IPSI administration inter-operates with Communication Manager Release 5.0 or earlier by using the pre-existing QoS and administration interface. An IPSI uses the IPSI administration feature if IPSI firmware version is 46 or greater, SIPI firmware version is 16 or greater, and Communication Manager system supports Release 5.2 features.

The IPSI administration feature with Communication Manager Release 5.2 works with earlier IPSI boards as described in the following:

- Communication Manager assesses the administration capability of an IPSI board based on the capabilities exchange message.
- In general, if an older IPSI is unable to support this feature, then that IPSI needs to be administered using the CLI interface. If Communication Manager is not able to exchange the capabilities message with an older IPSI board, the following happens:
  - Communication Manager stops sending any IPSI QoS or Ethernet settings to the IPSI.
  - Communication Manager stops receiving the IPSI QoS or the Ethernet settings from IPSI.
  - The IPSI reports its status on the IP Server Interface screen.

About the MM760 VoIP Media Module

The Avaya MM760 Media Module is a clone of the motherboard VoIP engine.The MM760 provides the audio bearer channels for voice over IP calls, and is under control of the G700. Based on system administration of audio codecs, a 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, the MM760 can service 64 channels. If any other codec type (G.723-5.3K, G.723-6.3K, or G.729) is administered, the 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 non-blocking system must add an additional MM760 Media Module, if they use more than two MM710 Media Modules in a single chassis. The additional MM760 provides an additional 64 channels and is supported by only G700 Media Gateway. The MM760 is ***not*** supported by G250, G350, G430 and G450 Media Gateways.

MM760 Ethernet interface

The MM760 must have its own Ethernet address. The MM760 requires a 10/100 Base T Ethernet interface to support H.323 endpoints for Avaya IP trunks and stations from another G700 Media Gateway. The MM760 is supported by only G700 Media Gateway. The MM760 is ***not*** supported by G250, G350, G430 and G450 Media Gateways.

Voice compression on the MM760

The MM760 supports on-board resources for compression and decompression of voice for G.711 (A- and µ-law), G.729 and 729B, and G.723 (5.3K and 6.3K). 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

The MM760 also supports transport of the following:

- Teletypewriter device (TTY) tone relay over the Internet
- Faxes over a corporate IP intranet

  Note:

  The path between endpoints for FAX transmissions must use Avaya telecommunications and networking equipment.

  ⚠ **SECURITY ALERT:**

  Faxes sent to non-Avaya endpoints cannot be encrypted.

- Modem tones over a corporate IP intranet

  Note:

  The path between endpoints for modem tone transmissions must use Avaya telecommunications and networking equipment.

About the Processor Ethernet

For more information about Processor Ethernet, see Processor Ethernet (PE) section of the Networking overview chapter.

SIP Direct Media

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

SIP Direct Media provides the following enhancements to SIP calls:

- Eliminates shuffling of SIP calls after call connects.
- Eliminates clipping on the talk path.

- Reduces the number of signalling messages for each SIP call.
- Reduces Communication Manager processing for each SIP call and increases the capacity of Communication Manager, Session Manager, and SIP Busy Hour Call Completion(BHCC).

For more information on enabling SIP Direct Media, see *Avaya Aura* ^{TM} *Communication Manager Feature Description and Implementation*, 555-245-205.

Administering Avaya gateways

The following document has additional information about the administration of the Avaya gateways:

- *Administering Avaya Aura™ Communication Manager* (03-300509).

Administering IP trunks

The following sections describe the administration of IP trunks:

- Administering SIP trunks
- Administering H.323 trunks

Administering SIP trunks

SIP is the Session Initiation Protocol, an endpoint-oriented messaging standard defined by the Internet Engineering Task Force (IETF). SIP "trunking" functionality is available on any of the Linux-based servers. These servers function as Plain Old Telephone Service (POTS) gateways, and they also support name/number delivery between and among the various non-SIP endpoints supported by Communication Manager (analog, DCP or H.323 stations and analog, digital or IP trunks), and SIP-enabled endpoints, such as the Avaya 4600-series SIP Telephones. In addition to its calling capabilities, IP Softphone R5 and later also includes optional instant-messaging client software, which is a SIP-enabled application, while continuing its full support of the existing H.323 standard for call control. Avaya SIP Softphone R2 and later releases fully support SIP for voice call control, as well as instant messaging and presence.

QSIG over SIP

You can use the QSIG over SIP(Q-SIP) feature to enable calls between two Communication Manager systems interconnected by an IP network that uses SIP signalling with the full range of QSIG functionality. For more information on QSIG over SIP, see *Avaya Aura ^{TM} Communication Manager Feature Description and Implementation, 555-245-205*.

Administering H.323 trunks

H.323 trunks use an ITU-T IP standard for LAN-based multimedia telephone systems. IP-connected trunks allow trunk groups to be defined as ISDN-PRI-equivalent tie lines 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 other vendors' H.323 v2-compliant switches
- Direct-inward-dial (DID) type public trunks, providing access to the switch for unregistered users

Setting up H.323 trunks for administration

This section describes the preliminary administration steps needed to set up H.323 trunks. Before you can administer an H.323 trunk, perform the following tasks:

- Verifying customer options for H.323 trunking
- Administering C-LAN and IP Media Processor circuit packs

  Note:

  These circuit packs are not required if your system has built-in Ethernet capabilities (S8300D).

- Administering QoS parameters
- Assigning IP node names and IP addresses
- Defining IP interfaces (C-LAN, TN2302AP, or TN2602AP Load Balanced)
- Assigning link through Ethernet data module
- Implementing Best Service Routing (optional)

Verifying customer options for H.323 trunking

Verify that H.323 trunking is set up correctly on the **system-parameters customer-options** screen. If any changes need to be made to fields on this screen, call your Avaya representative for more information.

To verify customer options for H.323 trunking:

1. Type **`display system-parameters customer-options`**, and go to the **Optional Features** screen.
2. Verify that the following fields have been completed on pages 1 and 2 of this screen:

Field	Conditions/Comments
G3 Version	This value should reflect the current version of Communication Manager.
Maximum Administered H.323 Trunks	Number of trunks purchased. Value must be greater than 0. On Page 2 of the screen.
Maximum Administered Remote Office Trunks	Number of remote office trunks purchased. This is also located on page 2 of the screen.

3. Go to the page that displays the **IP trunks** and **ISDN-PRI** fields.
4. Verify that **IP Trunks** and **ISDN-PRI** are enabled.

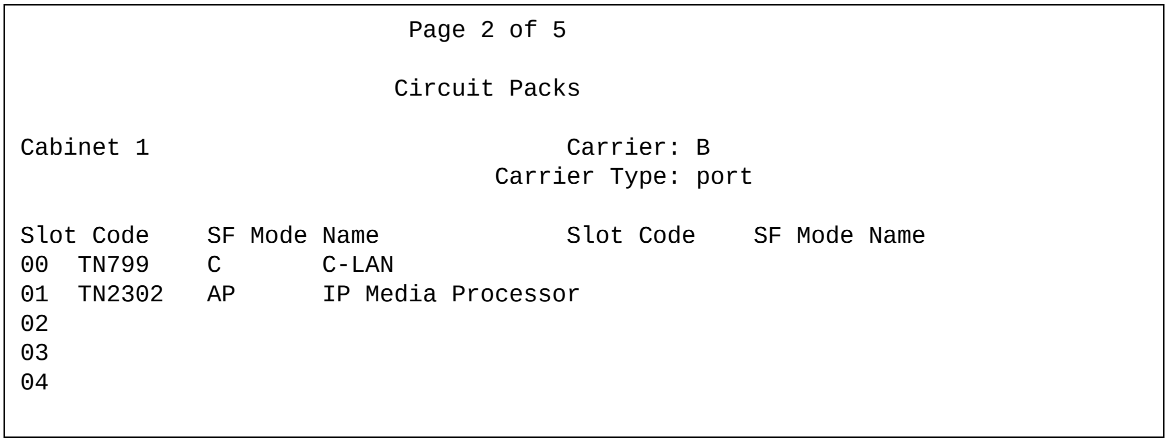
   If not, you need to obtain a new license file.

Administering C-LAN and IP Media Processor circuit packs

To administer the C-LAN and IP Media Processor circuit packs:

1. Type **`change circuit-packs`** to open the **Circuit Packs** screen.

Circuit Packs screen



```
                           Page 2 of 5

                          Circuit Packs

Cabinet 1                             Carrier: B
                                 Carrier Type: port

Slot Code    SF Mode Name             Slot Code    SF Mode Name
00  TN799    C       C-LAN
01  TN2302   AP      IP Media Processor
02
03
04
```

2. To administer a C-LAN circuit pack, complete the following fields:

Fields for C-LAN	Conditions/Comments
Code	**TN799DP**
Name	**C-LAN (**displays automatically)

3. To administer an IP Media Processor, complete the following fields:

x

Fields for IP Media	Conditions/Comments
Code	**TN2302AP** or **TN2602AP**
Name	**IP Media Processor** (displays automatically)

4. Submit the screen.

Administering 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 them to fit the needs of your network. (See Setting network performance thresholds).

Administer additional QoS parameters, including defining IP Network Regions and specifying the codec type to be used. See Chapter 5: Voice and Network quality administration.

Defining IP interfaces (C-LAN, TN2302AP, or TN2602AP Load Balanced)

The IP interface for each C-LAN, TN2302AP Media Processor, or TN2602AP (load-balanced) circuit pack on the switch must be defined on the **IP Interfaces** screen. Each switch in an IP network has one **IP Interfaces** screen.

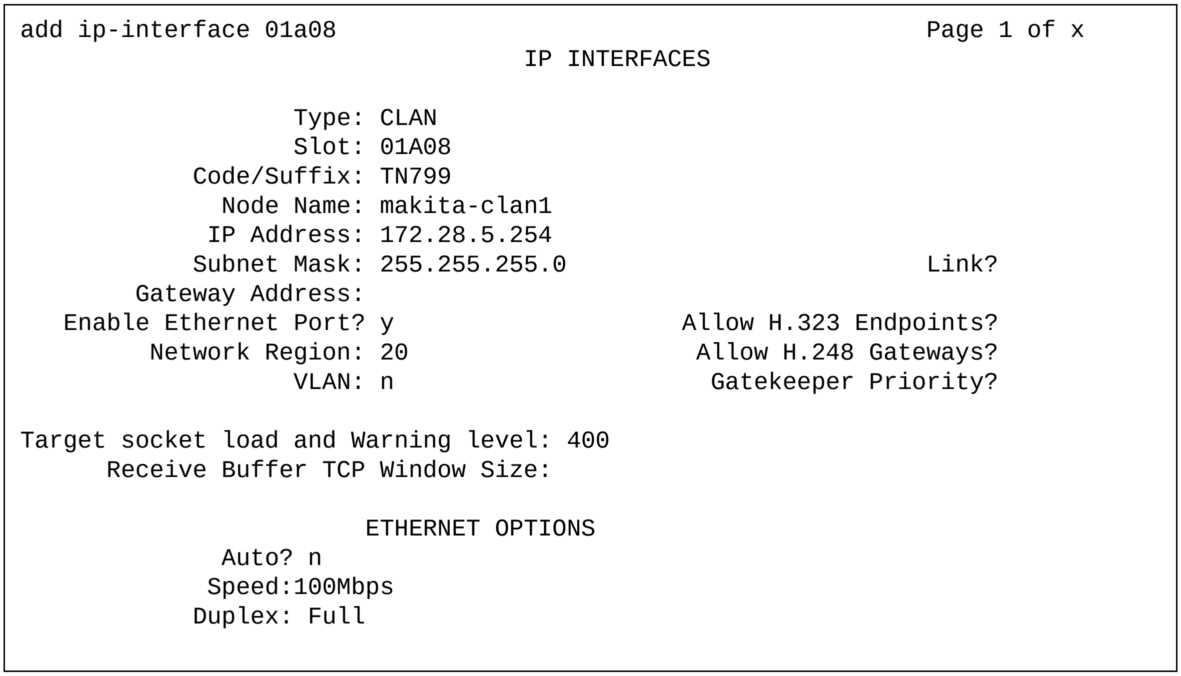
To define IP interfaces for each C-LAN and Media Processor circuit pack:

1. Type **`add ip-interface`** ***`CCccss`*** or ***`procr`*** to open the **IP Interfaces** screen.

   Note:

   This screen shows the display for the servers.

IP Interfaces screen



```
add ip-interface 01a08                                         Page 1 of x
                                   IP INTERFACES

                   Type: CLAN
                   Slot: 01A08
            Code/Suffix: TN799
              Node Name: makita-clan1
             IP Address: 172.28.5.254
            Subnet Mask: 255.255.255.0                         Link?
        Gateway Address:
   Enable Ethernet Port? y                    Allow H.323 Endpoints?
         Network Region: 20                    Allow H.248 Gateways?
                   VLAN: n                      Gatekeeper Priority?

Target socket load and Warning level: 400
      Receive Buffer TCP Window Size:

                        ETHERNET OPTIONS
              Auto? n
             Speed:100Mbps
            Duplex: Full
```

2. Complete the following fields as shown:

Field	Conditions/Comments
Critical Reliable Bearer	Appears only for the TN2602AP. Type **n** when the TN2602AP is in load balancing mode or is the only TN2602AP circuit pack in the port network.
Type	Display only. This field is automatically populated with **C-LAN, MEDPRO,** or **PROCR**. The fields differ on the screens for each of the IP Interface types. Required entries may also differ for Processor Ethernet (PE). See the Screen Reference chapter of the *Administering Avaya Aura™ Communication Manager,* 03-300509.
Slot	Display only. The slot location for the circuit pack.
Code/Suffix	Display only. This field is automatically populated with TN799DP for C-LAN, TN2302AP for IP Media Processor, or TN2602AP for IP Media Resource 320, and the suffix letter(s).
Node name	The node name for the IP interface. This node name must already be administered on the **IP Node Names** screen.
IP Address	Display only. The IP address for this IP interface. The IP address is associated with the node name on the **IP Node Names** screen.

Field	Conditions/Comments
Subnet Mask	The subnet mask associated with the IP address for this IP interface.
Link?	Display only. Shows the administered link number for an Ethernet link. See Assigning link through Ethernet data module on page 69
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.
Enable Ethernet Port?	Enter **y**
Allow H.323 Endpoints?	Controls whether IP endpoints can register on the interface. On a single main server, enter **y** to allow H.323 endpoint connectivity to the PE interface. Enter **n** if you do not want H.323 endpoint connectivity to the PE interface. **Note:** For a Survivable Core server, this field is display-only and is set to **n**. H.323 endpoint connectivity using the PE interface on a Survivable Core server is not supported. For a Survivable Remote Server, this field is display-only and is set to **y**.
Network Region	The region number for the IP interface. Enter a value between **1-250**
Allow H.248 Gateways?	Controls whether H.248 media gateways (G700, G450, G430, G350, G250) can register on the interface. On a single main server, enter **y** to allow H.248 endpoint connectivity to the PE interface. Enter **n** if you do not want H.248 endpoint connectivity to the PE interface. **Note:** For an Survivable Core Server, this field is display-only and is set to **n**. H.248 endpoint connectivity using the PE interface on an ESS server is not supported. For a Survivable Remote server, this field is display-only and is set to **y**.
VLAN	The 802.1Q virtual LAN value (**0 - 4094**) or **n** (no VLAN). This VLAN field interfaces with the TN799 (C-LAN) or TN802B Media Processor circuit packs; it does not send any instructions to IP endpoints.
Gatekeeper Priority?	Appears only if **Allow H.323 Endpoints** is **y** and the Communication Manager server is a main server or an Survivable Remote server. This field does not display on an Survivable Core server. This field allows a priority to be set on the interface. This affects where the interface appears on the gatekeeper list. Enter the desired priority number, a value from **1** to **9**. The value in this field is used on the alternate gatekeeper list. The lower the number, the higher the priority. Default is **5**.

Field	Conditions/Comments
VOIP Channels	Appears only for a TN2602AP circuit pack. Enter the number of VoIP channels assigned to the TN2602AP circuit pack, either **0**, **80**, or **320**. **0** means the circuit pack will not be used. **Note:** If two TN2602 circuit packs in a port network are administered for 320 channels, only 512 channels are used due to the 512 TDM timeslot maximum for a port network. The system-wide number of TN2602 circuit packs administered for 80 channels cannot exceed the number of 80-channel licenses installed on system. Similarly, the number of TN2602 circuit packs administered for 320 channels cannot exceed the number of 320-channel licenses installed on the system.
Target socket load and Warning level	Always leave the default (**400**) unless instructed to enter a different value (**1** to **499**) by Avaya Services.
Receive Buffer TCP Window Size	A value of **512** to **8320**
Auto? Speed Duplex	Set Ethernet Options to match the customers network. The recommended settings are: ● Auto? **n** If you set Auto to **n**, also complete the following fields. The recommended values are displayed. ● Speed: **100 Mbps** ● Duplex: **Full** See *IP Telephony Implementation Guide*, for a discussion of the Ethernet Options settings.

3. Submit the screen.

Defining IP interfaces (duplicated TN2602AP)

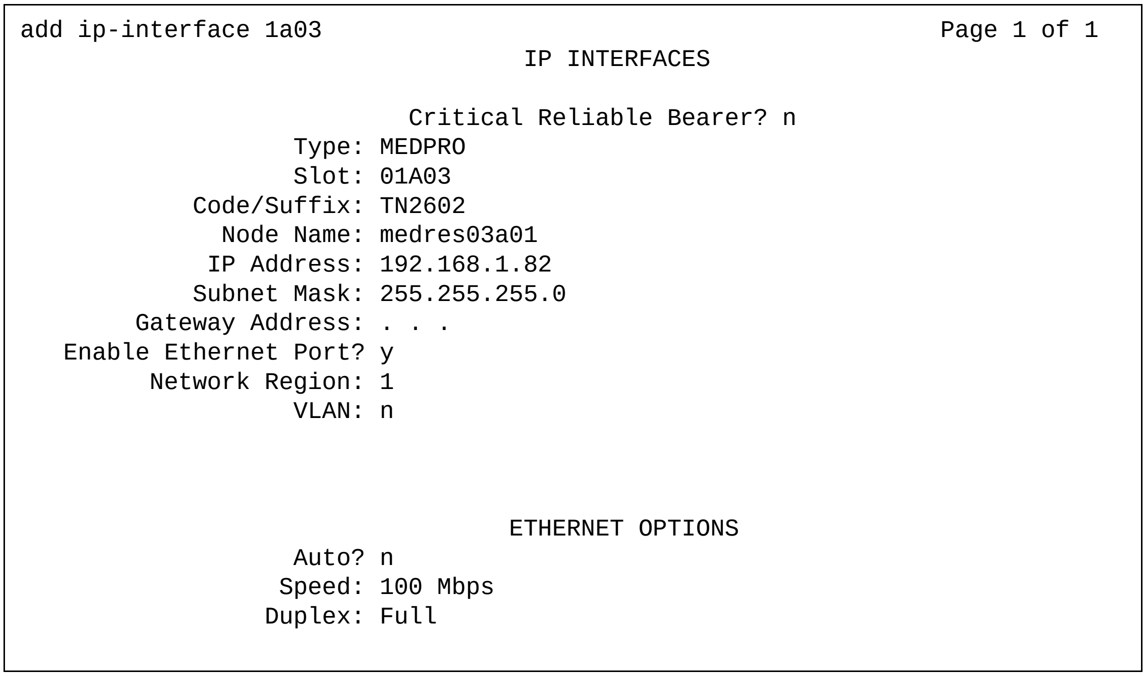
To define IP interfaces for duplicate TN2602AP Media Resource 320 circuit packs:

1. Type **`add ip-interface`** ***`CCccss`*** to open the **IP Interfaces** screen.

   The IP Interfaces screen appears.

Note:

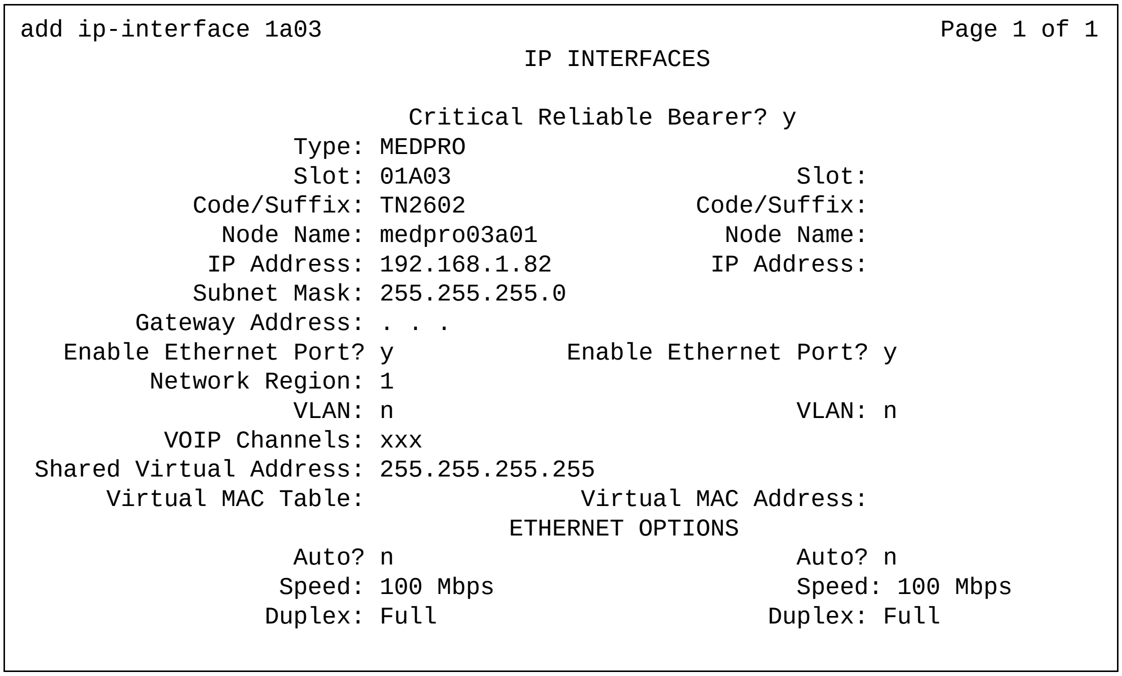
This screen shows the display for the servers.



```
add ip-interface 1a03                                           Page 1 of 1
                                   IP INTERFACES

                           Critical Reliable Bearer? n
                   Type: MEDPRO
                   Slot: 01A03
            Code/Suffix: TN2602
              Node Name: medres03a01
             IP Address: 192.168.1.82
            Subnet Mask: 255.255.255.0
        Gateway Address: . . .
   Enable Ethernet Port? y
         Network Region: 1
                   VLAN: n



                                  ETHERNET OPTIONS
                   Auto? n
                  Speed: 100 Mbps
                 Duplex: Full
```

2. In the **Critical Reliable Bearer?** field, type **y**, and press **Enter**.

   A second column of data for a standby TN2602AP appears on the right of the screen.



```
add ip-interface 1a03                                           Page 1 of 1
                                   IP INTERFACES

                           Critical Reliable Bearer? y
                   Type: MEDPRO
                   Slot: 01A03                        Slot:
            Code/Suffix: TN2602                Code/Suffix:
              Node Name: medpro03a01             Node Name:
             IP Address: 192.168.1.82           IP Address:
            Subnet Mask: 255.255.255.0
        Gateway Address: . . .
   Enable Ethernet Port? y            Enable Ethernet Port? y
         Network Region: 1
                   VLAN: n                            VLAN: n
          VOIP Channels: xxx
 Shared Virtual Address: 255.255.255.255
      Virtual MAC Table:               Virtual MAC Address:
                                  ETHERNET OPTIONS
                   Auto? n                            Auto? n
                  Speed: 100 Mbps                     Speed: 100 Mbps
                 Duplex: Full                       Duplex: Full
```

3. Complete the following fields as shown:

Field	Conditions/Comments
Type	Display only. This field is automatically populated with **MEDPRO**.
Slot	Slot location entered in the command line. Enter the location of the second TN2602AP circuit pack for a non-duplicated board. The second (right-side) Slot field is automatically populated when Critical Reliable Bearer is **y.**
Code/Sfx	Circuit pack TN code and suffix. Display only for TN2602AP when Critical Reliable Bearer is **n.** The second (right-side) Code/Sfx field is automatically populated based on the corresponding Slot field information, when Critical Reliable Bearer is **y.**
Node name	The node name for the IP interface. This node name must already be administered on the **IP Node Names** screen.
IP Address	Display only. The IP address for this IP interface. The IP address is associated with the node name on the **IP Node Names** screen.
Subnet Mask	Enter the Subnet Mask for TN2602AP. This entry also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is **y**
Gateway Address	The IP address of the LAN gateway associated with the TN2602AP. This entry also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is **y**
Enable Ethernet Pt	**y**/**n** **y** = The Ethernet Port associated with the TN2602AP is in service. If this is an active board, set to **n** only when there is no standby, or when the standby has been disabled. **Note:** Note: You may be required to enter **n** in this field before you make changes to this screen.
Network Region	Number of the Network Region where the interface resides. This entry also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is **y**
VLAN	The 802.1Q virtual LAN value (**0 - 4094**) or **n** (no VLAN). This VLAN field interfaces with the media processor circuit packs; it does not send any instructions to IP endpoints.
	1 of 3

Field	Conditions/Comments
VOIP Channels	**0** (will not support voice calls) **80** (low density) **320** (standard) The number of VoIP channels that are allocated to the associated TN2602. Appears for a TN2602 circuit pack on Communication Manager 3.0/V13 or greater. This number also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is **y** Users will be blocked from administering 80 or 320 VoIP channels if there is no available capacity for the corresponding "Maximum TN2602 boards with 80 VoIP Channels"/"Maximum TN2602 boards with 320 VoIP Channels" license feature.
Shared Virtual Address	The virtual IP address shared by the two TN2602AP circuit packs, when duplicated. This address enables Communication Manager to connect endpoints through the TN2602AP circuit packs to the same address, regardless of which one is actually active. Appears when Critical Reliable Bearer is **y**.
Virtual MAC Table	**1** through **4**, default = **1** Table number where the virtual MAC address, shared by duplicated TN2602AP circuit packs, is obtained. Appears when Critical Reliable Bearer is **y**. You might choose a different table number other than **1** if all of the following conditions exist: ● A port network under the control of a different Communication Manager main server has duplicated TN2602AP circuit packs. ● That port network controlled by a different main server has the same number as the port network in which you are administering the TN2602AP circuit packs. ● The port network or its main server connects to the same Ethernet switch as the port network in which you are administering the TN2602AP circuit packs. Selecting a different Virtual MAC Table from that chosen for a port network that has the previously-listed conditions helps prevent the possibility that two TN2602AP circuit packs within the customer's network will have the same virtual MAC address.
	2 of 3

Field	Conditions/Comments
Virtual MAC Address	Virtual MAC address that is shared by duplicated TN2602AP circuit packs. Automatically populated based on the Virtual MAC address table. Appears when Critical Reliable Bearer is **y**.
Auto?	Set Ethernet Options to match the customers network. The recommended settings are: ● Auto? **n** If you set Auto to **n**, also complete the following fields. The recommended values are displayed. ● Speed: **100 Mbps** ● Duplex: **Full** See *IP Telephony Implementation Guide*, for a discussion of the Ethernet Options settings.
	3 of 3

4. Submit the screen.

Assigning link through Ethernet data module

Note:

The S8300D Server does not support data modules.

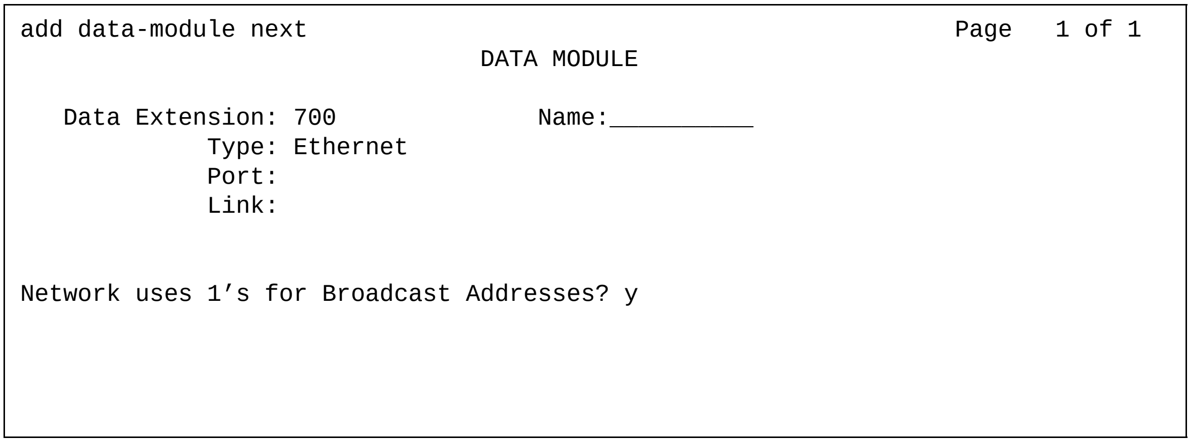
This section describes how to administer an Ethernet data module for the connection between the C-LAN circuit pack’s Ethernet port (port 17) and the LAN. The data module associates a link number and extension number with the C-LAN Ethernet port location. This association is used by the processor to set up and maintain signaling connections for multimedia call handling.

The C-LAN Ethernet port is indirectly associated with the C-LAN IP address through the slot location (which is part of the port location) on the **IP Interfaces** screen and the node name, which is on both the **IP Interfaces** and **Node Names** screens.

To assign a link through an Ethernet data module:

1. Type **`add data-module`** ***`next`*** to open the **Data Module** screen.

Data Module screen



```
add data-module next                                        Page   1 of 1
                                DATA MODULE

   Data Extension: 700              Name:__________
             Type: Ethernet
             Port:
             Link:


Network uses 1’s for Broadcast Addresses? y
```

2. Complete the following fields as shown:

Field	Conditions/Comments
Data Extension	Populated automatically with the **next** qualifier or type the extension number.
Type	Enter **Ethernet**. This indicates the data-module type for this link.
Port	Ethernet connections must be assigned to port **17** on the C-LAN circuit pack.
Link	Enter the link number, a link not previously assigned on this switch.
Name	Display only. The name appears in lists generated by the `list data module` command.
Network uses 1’s for broadcast addresses	Enter **y** if the private network contains only Avaya switches and adjuncts. Enter **n** if the network includes non-Avaya switches that use the 0’s method of forming broadcast addresses.

For more information on the fields that may appear on this screen, see the *Administering Avaya Aura™ Communication Manager,* 03-300509.

3. Submit the screen.

Implementing Best Service Routing (optional)

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

Avaya recommends that if H.323 trunks are used for BSR interflow, the traffic should be routed to a low-occupancy or unshared LAN/WAN segment. Alternatively, you might want to route internal interflow traffic, which may have lower quality-of-service requirements, over H.323 trunks, and route customer interflow traffic over circuit-switched tie trunks.

Completing H.323 trunk administration

In the previous sections, you have completed the pre-administration tasks to set up H.323 trunks (see Setting up H.323 trunks for administration). This section describes the tasks that you need to complete to administer an H.323 trunk. Sample values are used to populate the fields to show the relationships between the screens and fields. Perform the following tasks:

- Creating an H323 trunk signaling group

  Create a signaling group for the H.323 trunks that connect this switch to a far-end switch.
- Creating a trunk group for H.323 trunks
- Modifying the H.323 trunk signaling group

  Modify the signaling group by entering the H.323 trunk group number in the **Trunk Group for the Channel Selection** field of the **Signaling Group** screen.

Creating an H323 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.

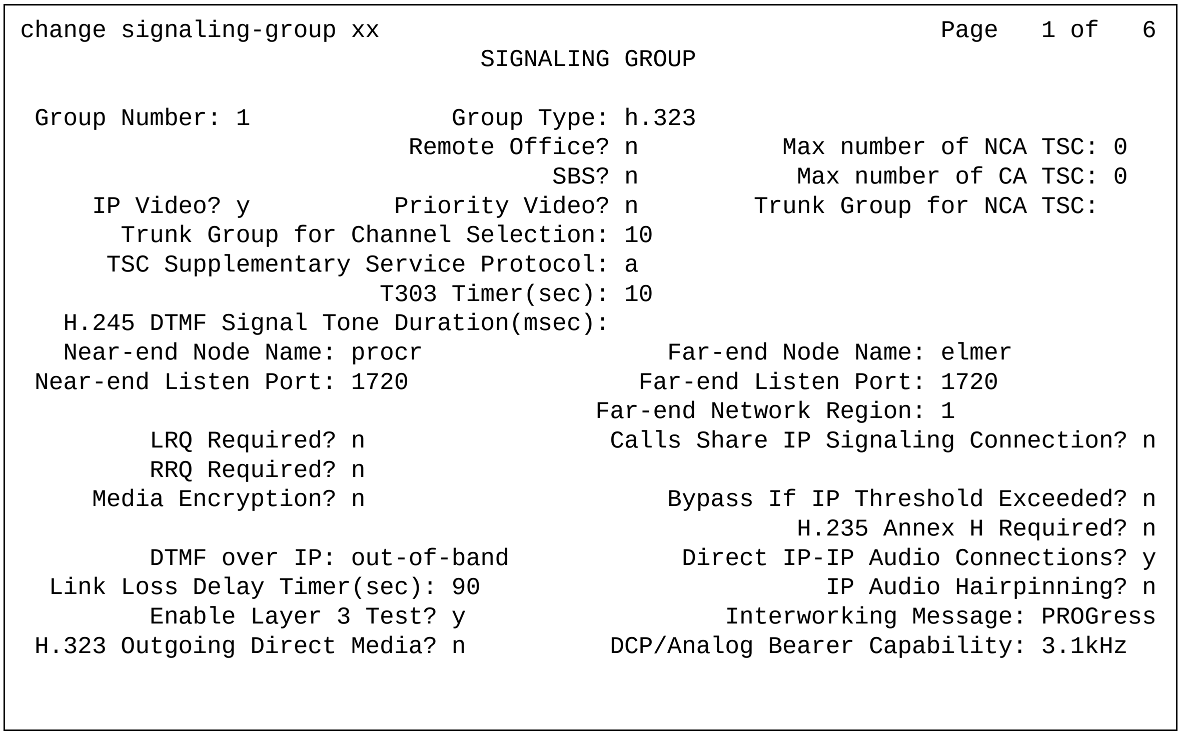
Note:

> The following steps address only those fields that are specifically related to H.323 trunks. The other fields are described in the *Administering Avaya Aura™ Communication Manager,* 03-300509.

To create an H.323 trunk signaling group, do the following:

1. Type **`add signaling-group`** ***`number`*** to open the **Signaling Group** screen.

Signaling Group screen



```
change signaling-group xx                                       Page   1 of   6
                                SIGNALING GROUP

 Group Number: 1              Group Type: h.323
                           Remote Office? n          Max number of NCA TSC: 0
                                     SBS? n           Max number of CA TSC: 0
     IP Video? y          Priority Video? n        Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 10
      TSC Supplementary Service Protocol: a
                         T303 Timer(sec): 10
   H.245 DTMF Signal Tone Duration(msec):
   Near-end Node Name: procr                 Far-end Node Name: elmer
 Near-end Listen Port: 1720                Far-end Listen Port: 1720
                                        Far-end Network Region: 1
         LRQ Required? n                 Calls Share IP Signaling Connection? n
         RRQ Required? n
     Media Encryption? n                     Bypass If IP Threshold Exceeded? n
                                                      H.235 Annex H Required? n
         DTMF over IP: out-of-band            Direct IP-IP Audio Connections? y
  Link Loss Delay Timer(sec): 90                        IP Audio Hairpinning? n
         Enable Layer 3 Test? y                  Interworking Message: PROGress
 H.323 Outgoing Direct Media? n          DCP/Analog Bearer Capability: 3.1kHz
```

2. Complete the following fields as shown:

Table 4: Signaling Group screen options

Field	Conditions/Comments
Group Type	Enter **h.323**
Trunk Group for Channel Selection	Leave blank until you create a trunk group in the following task, then use the change command and enter the trunk group number in this field.
T303 Timer	Use this field to enter the number of seconds the system waits for a response from the far end before invoking Look Ahead Routing. Appears when the Group Type field is isdn-pri (DS1 Circuit Pack screen) or h.323 (Signaling Group screen).
H.245 DTMF Signal Tone Duration (msec)	This field specifies the tone duration of DTMF tones sent in H.245-signal message when **DTMF over IP:** field is set to **out-of-band** on the **Signaling Group screen** for IP Trunks. The value of this field can be either in the range 80 ms to 350 ms or blank. The default Value is blank.

1 of 4

Table 4: Signaling Group screen options (continued)

Field	Conditions/Comments
Near-end Node Name	Enter 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.
Far-end Node Name	This is 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 blank when the signaling group is associated with an unspecified destination.
Near-end Listen Port	Enter an unused port number from the range **1719**, **1720** or **5000–9999**. Avaya recommends **1720**. If the **LRQ** field is **y**, enter **1719**.
Far-end Listen Port	Enter the same number as the one in the **Near-end Listen Port** field. This number must match the number entered in the **Near-end Listen Port** field on the Signaling Group screen for the far-end switch. Leave blank when the signaling group is associated with an unspecified destination.
Far-end Network Region	Identify 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 instead of the default region (obtained from the C-LAN used by the signaling group) for selection of a codec. Enter a value between **1-250**. Leave blank to select the region of the near-end node (C-LAN).
LRQ Required	Enter **n** when the far-end switch is an Avaya product and H.235 Annex H Required? is set to **n**. Enter **y** when: ● H.235 Annex H Required? is set to **y**, or ● the far-end switch requires a location request to obtain a signaling address in its signaling protocol.
Calls Share IP Signaling Connection	Enter **y** for connections between Avaya equipment. Enter **n** when the local and/or remote switch is not Avaya’s.
RRQ Required	Enter **y** when a vendor registration request is required.
Bypass if IP Threshold Exceeded	Enter **y** to automatically remove from service trunks assigned to this signaling group when IP transport performance falls below limits administered on the **Maintenance-Related System Parameters** screen.

2 of 4

Table 4: Signaling Group screen options (continued)

Field	Conditions/Comments
H.235 Annex H Required	Enter **y** to indicate that the CM server requires the use of H.235 amendment 1 with annex H protocol for authentication during registration.
DTMF Over IP	Signifies 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.
Direct IP-IP Audio Connections	Allows direct audio connections between H.323 endpoints. For SIP trunk groups, this is the value that allows direct audio connections between SIP endpoints. Enter a **y** to save on bandwidth resources and improve sound quality of voice over IP (VoIP) transmissions.
Link Loss Delay Timer	Use this field to 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 (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
IP Audio Hairpinning	The **IP Audio Hairpinning** field entry allows the option for H.323 endpoints and SIP endpoints to be connected through the IP circuit pack in the server or switch, without going through the time division multiplexing (TDM) bus. Type **y** to enable hairpinning for H.323 groups. Default is **n**.

3 of 4

Table 4: Signaling Group screen options (continued)

Field	Conditions/Comments
Interworking Message	This field determines what message Communication Manager sends when an incoming ISDN trunk call interworks (is routed over a non-ISDN trunk group). Normally select the value, **PROGress**, which asks the public network to cut through the B-channel and let the caller hear tones such as ringback or busy tone provided over the non-ISDN trunk. 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 interworks to a non-ISDN trunk.
DCP/Analog Bearer Capability	This field sets the information transfer capability in a bearer capability IE of a setup message to **speech** or **3.1kHz**. The latter is the default. 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.
	4 of 4

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

   Enter NCA TSC information on this screen according the detailed descriptions contained in the Screen Reference chapter of the *Administering Avaya Aura™ Communication Manager,* 03-300509.

4. Submit the screen.

Creating a trunk group for H.323 trunks

This task creates a new trunk group for H.323 trunks. Each H.323 trunk must be a member of an ISDN trunk group and must be associated with an H.323 signaling group.

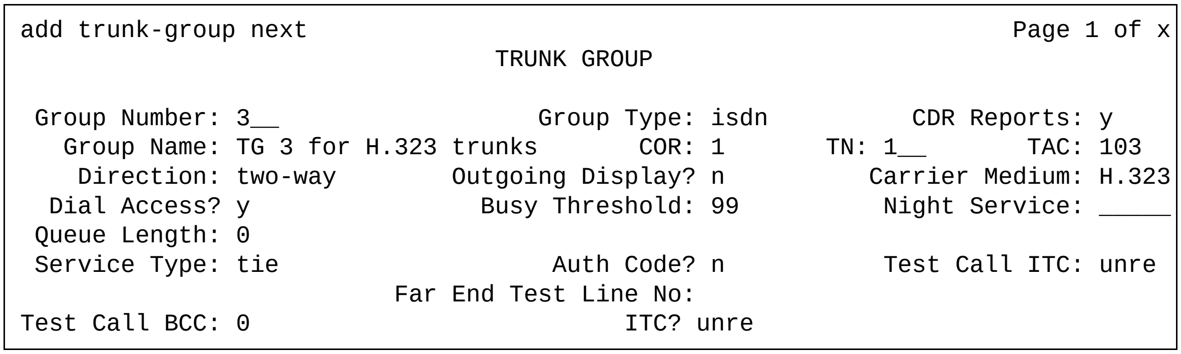
Note:

> The following steps address only those fields that are specifically related to H.323 trunks. The other fields are described in the *Administering Avaya Aura™ Communication Manager,* 03-300509.

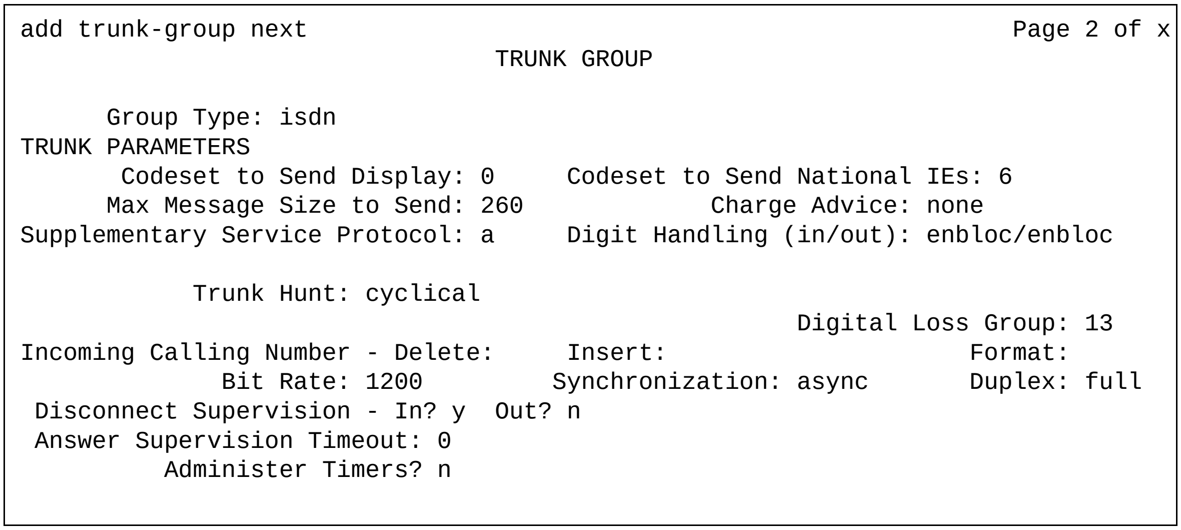
To create an ISDN trunk group, do the following:

1. Type **`add trunk-group`** ***`next`*** to open the **Trunk Group** screen.

Trunk Group screen



```
add trunk-group next                                                 Page 1 of x
                                 TRUNK GROUP

 Group Number: 3__                  Group Type: isdn          CDR Reports: y
   Group Name: TG 3 for H.323 trunks       COR: 1       TN: 1__       TAC: 103
    Direction: two-way        Outgoing Display? n          Carrier Medium: H.323
  Dial Access? y                Busy Threshold: 99          Night Service: _____
 Queue Length: 0
 Service Type: tie                   Auth Code? n           Test Call ITC: unre
                          Far End Test Line No:
Test Call BCC: 0                          ITC? unre
```



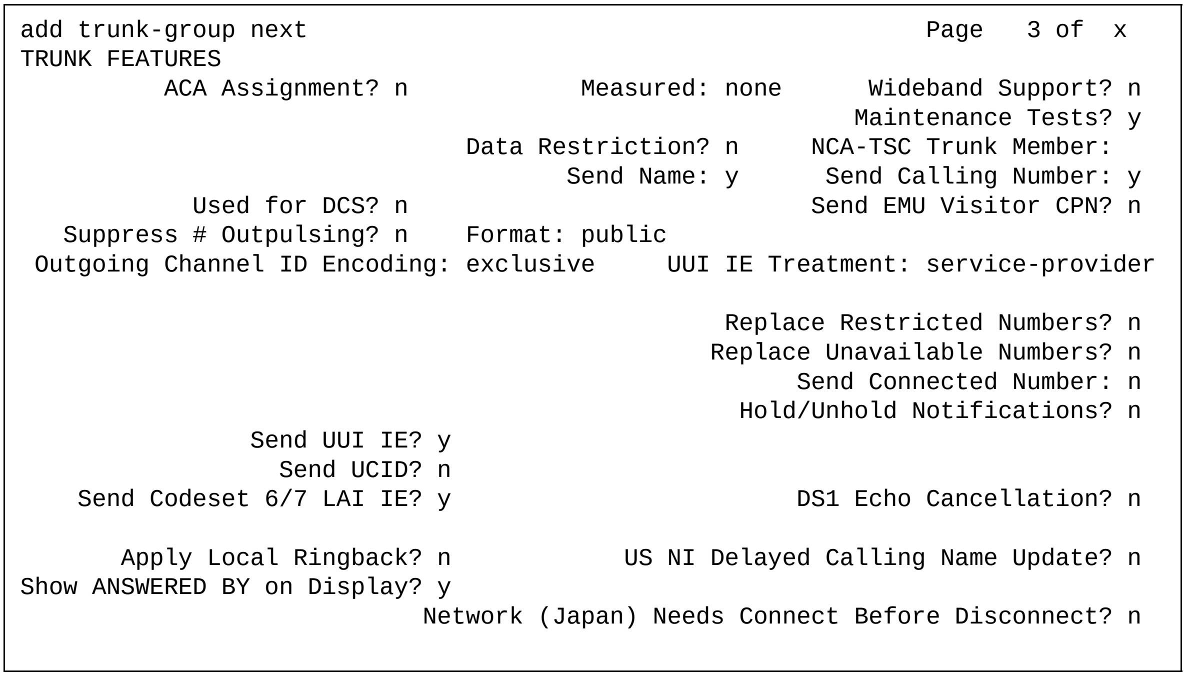
```
add trunk-group next                                                 Page 2 of x
                                 TRUNK GROUP

      Group Type: isdn
TRUNK PARAMETERS
       Codeset to Send Display: 0     Codeset to Send National IEs: 6
      Max Message Size to Send: 260             Charge Advice: none
Supplementary Service Protocol: a     Digit Handling (in/out): enbloc/enbloc

            Trunk Hunt: cyclical
                                                      Digital Loss Group: 13
Incoming Calling Number - Delete:     Insert:                     Format:
              Bit Rate: 1200         Synchronization: async       Duplex: full
 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 0
          Administer Timers? n
```

2. Complete the following fields as shown:

Field	Conditions/Comments
Group Type	Enter **isdn**
Carrier Medium	Enter **H.323**
Service Type	Enter **tie**
TestCall ITC	Enter **unre** (unrestricted).
TestCall BCC	Enter **0**
Codeset to Send Display	Enter **0**
Outgoing Display	This field might need to be changed if the far-end is not Avaya's.

3. Go to the **Trunk Features** page of this screen.

Trunk Features screen

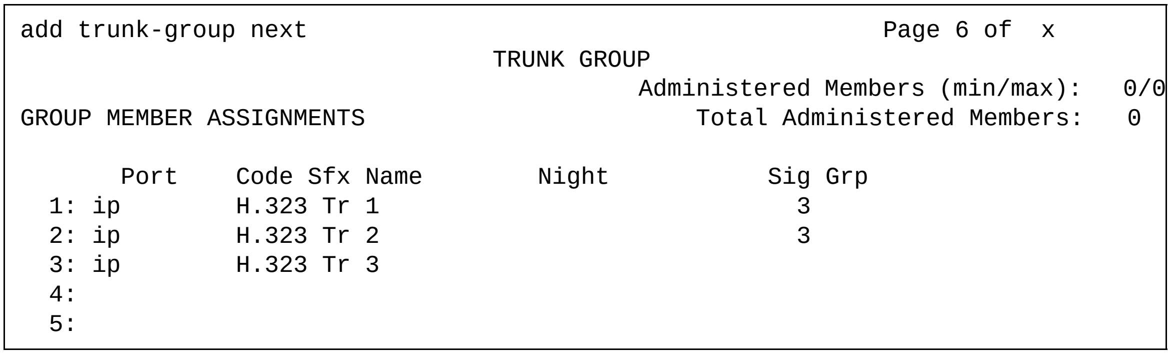


```
add trunk-group next                                           Page   3 of  x
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                                          Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                      Send Name: y      Send Calling Number: y
            Used for DCS? n                            Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: public
 Outgoing Channel ID Encoding: exclusive     UUI IE Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                                      Send Connected Number: n
                                                  Hold/Unhold Notifications? n
                Send UUI IE? y
                  Send UCID? n
    Send Codeset 6/7 LAI IE? y                        DS1 Echo Cancellation? n

       Apply Local Ringback? n           US NI Delayed Calling Name Update? n
Show ANSWERED BY on Display? y
                            Network (Japan) Needs Connect Before Disconnect? n
```

4. Complete the following fields as shown:

Field	Conditions/Comments
Send Name Send Calling Number Send Connected Number	If **y** is entered, either the **ISDN Numbering - Public/Unknown Format** screen, or the **ISDN Numbering - Private** screen (based on the **Format** field) is accessed to construct the actual number to be sent to the far end.

5. To add a second signaling group, go to the **Group Member Assignments** page of this screen.



```
add trunk-group next                                        Page 6 of  x
                                 TRUNK GROUP
                                           Administered Members (min/max):   0/0
GROUP MEMBER ASSIGNMENTS                       Total Administered Members:   0

       Port    Code Sfx Name        Night           Sig Grp
  1: ip        H.323 Tr 1                             3
  2: ip        H.323 Tr 2                             3
  3: ip        H.323 Tr 3
  4:
  5:
```

Note:

Each signaling group can support up to 255 trunks. If you need more than 31 trunks between the same two switches, add a second signaling group with different listen ports and add the trunks to the existing or second trunk group.

6. Enter group numbers using the following fields:

Field	Conditions/Comments
Port	Enter **ip**. When the screen is submitted, this value is automatically changed to a **T** number (**Txxxxx**).
Name	Enter a 10-character name to identify the trunk.
Sig Grp	Enter the number for the signaling group associated with this H.323 trunk.

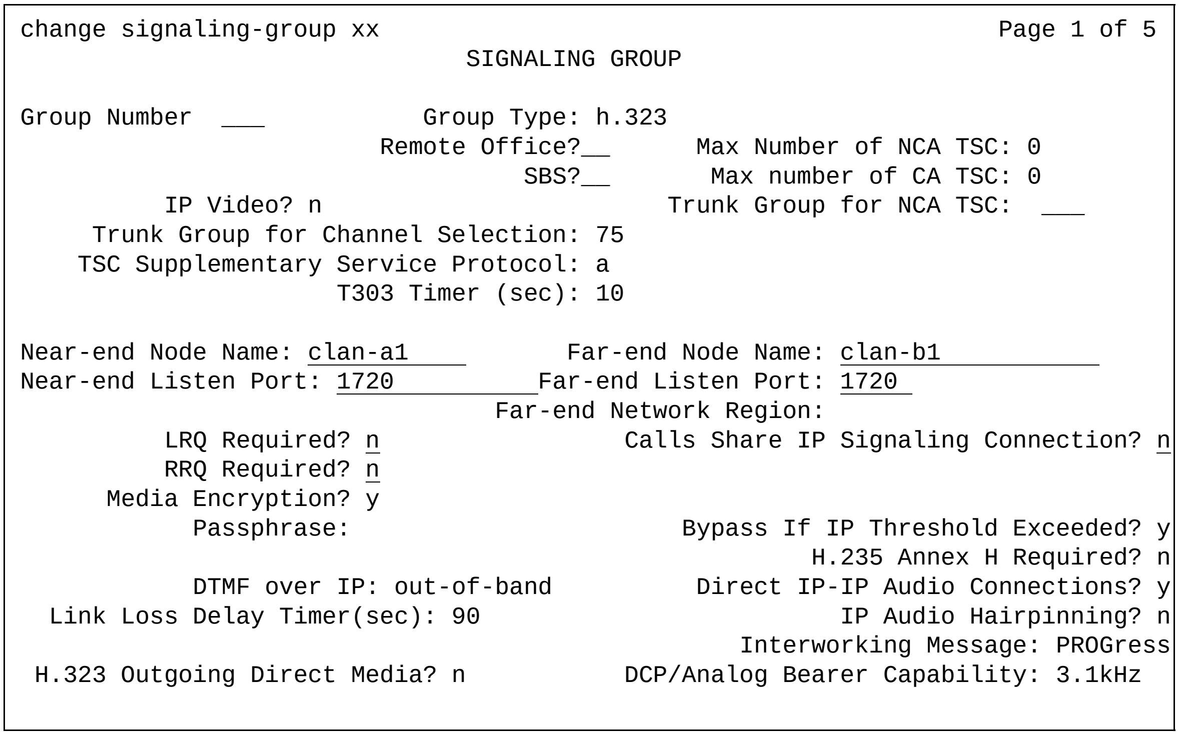
Modifying the H.323 trunk signaling group

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

To modify an H.323 trunk signaling group:

1. Type **busy signaling-group** ***number*** to busy-out the signaling group.
2. Type **change signaling-group** ***number*** to open the **Signaling Group** screen.

Signaling Group screen



```
change signaling-group xx                                           Page 1 of 5
                               SIGNALING GROUP

Group Number  ___           Group Type: h.323
                         Remote Office?__      Max Number of NCA TSC: 0
                                   SBS?__       Max number of CA TSC: 0
          IP Video? n                        Trunk Group for NCA TSC:  ___
     Trunk Group for Channel Selection: 75
    TSC Supplementary Service Protocol: a
                      T303 Timer (sec): 10

Near-end Node Name: clan-a1           Far-end Node Name: clan-b1
Near-end Listen Port: 1720          Far-end Listen Port: 1720
                                 Far-end Network Region:
          LRQ Required? n                 Calls Share IP Signaling Connection? n
          RRQ Required? n
      Media Encryption? y
            Passphrase:                       Bypass If IP Threshold Exceeded? y
                                                       H.235 Annex H Required? n
            DTMF over IP: out-of-band                Direct IP-IP Audio Connections? y
  Link Loss Delay Timer(sec): 90                               IP Audio Hairpinning? n
                                                  Interworking Message: PROGress
 H.323 Outgoing Direct Media? n           DCP/Analog Bearer Capability: 3.1kHz
```

3. Complete the following field:

Field	Conditions/Comments
Trunk Group for Channel Selection	Enter the trunk group number. If there is more than one trunk group assigned to this signaling group, the group entered in this field is the group that accepts incoming calls.

4. Submit the screen.

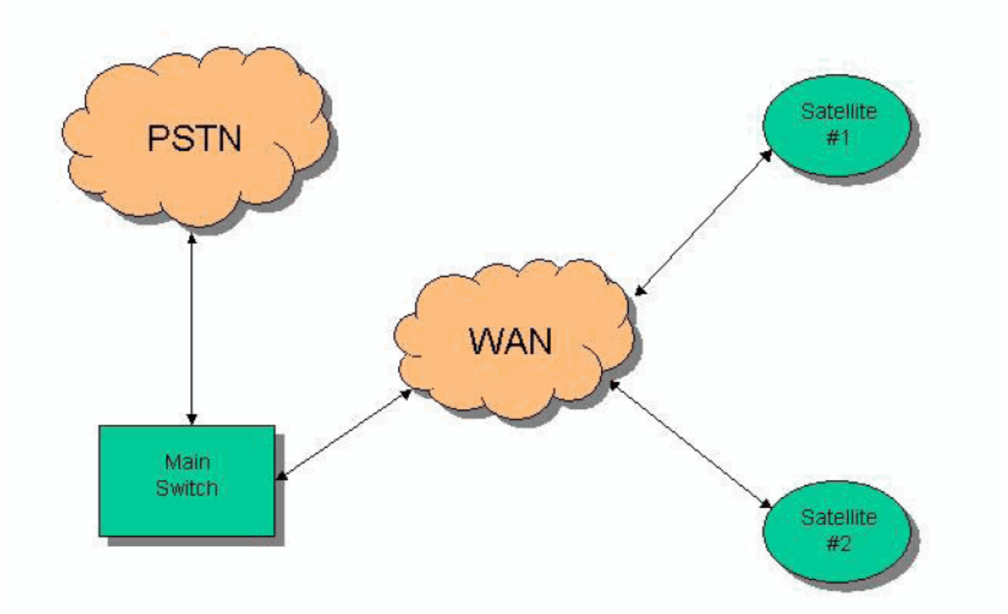
5. Type **`release signaling-group`** ***`number`*** to release the signaling group.

Dynamic generation of private/public calling party numbers

Often it is necessary to generate a private Calling Party Number (CPN) for calls within a network, but a public CPN for calls that route through the main network switch to the PSTN.

Consider a network such as the following:

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)), but when any node dials the PSTN, to route the call 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**. (The value **unk-pvt** means "encode the number as an "unknown" type of number, but use the **Numbering-Private Format** screen to generate the actual number.)

Note:

IP trunks function as ISDN trunks in this respect.

In the network example, the system only generates a Private CPN if the caller dials a Private (level 0/1/2) or Unknown (unk-unk) number. If the caller dials a Public number, the system generates a Public CPN. It is necessary to fill out the **Numbering-Private Format** and **Numbering-Public/Unknown Format** forms appropriately, and then to 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 0/1/2) either on the **AAR Analysis** screen or on the **Route Pattern** screen, but you can only designate the type of number as Unknown (**unk-unk**) on the **Route Pattern** screen. If the customer uses UDP, Unknown is the better Type of Number to use.

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, the recommended way is to set the **Numbering Format** to **unk-unk** on the **Route Pattern** screen.

Administering Avaya phones

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

- Administering IP Softphones
- Installing and administering Avaya IP telephones

Administering IP Softphones

IP Softphones operate on a PC equipped with Microsoft Windows and with TCP/IP connectivity through Communication Manager. Avaya offers the following Softphone applications:

- IP Softphone for any phone user
- IP Agent for call center agents
- Softconsole for console attendants
- One-X Communicator
- SIP softphone
- one-X Portal as software-only phone

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

- **Road-warrior** mode consists of a PC 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 PC 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 that will allow an IP Softphone and a non-Softphone telephone to be in service on the same extension at the same time. In this new configuration, the call control is provided by both the Softphone and the telephone endpoint. The audio is provided by the telephone endpoint.

Documentation on how to set up and use the IP Softphones is included on the CD-ROM containing the IP Softphone software. Procedures for administering Communication Manager to support IP Softphones are given in *Administering Avaya Aura™ Communication Manager,* 03-300509*.*

This section focuses on administration for the trunk side of the Avaya IP Solutions offer, plus a checklist of IP Softphone administration. Comprehensive information on the administration of IP Softphones is given in *Administering Avaya Aura™ Communication Manager,* 03-300509.

There are two main types of IP Softphone configurations:

- Administering a Telecommuter phone
- Administering a Road-warrior phone

Communication Manager can distinguish between various IP stations at registration using the product ID and release number sent during registration. An IP phone with an Avaya manufacturer ID can register if the number of stations with the same product ID and the same or lower release number *is less than* the administered system capacity limits. System limits are based on the number of simultaneous registrations. Note that a license is required for each station that is to be IP softphone enabled.

Administering a Telecommuter phone

The Telecommuter uses two connections: one to the PC over the IP network and another connection to the telephone over the PSTN. IP Softphone PC 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. The *init* login does not have the ability to change the customer options, offer options, or special applications screens.

To administer a Telecommuter phone:

1. Type **`display system-parameters customer-options`** and press **Enter** to open the **System Parameters Customer Options** screen.

   Verify that IP Softphone is enabled. Review the following fields on the screen:

Field	Value
Maximum Concurrently Registered IP Stations	Identifies the maximum number of IP stations that are simultaneously registered, not the maximum number that are simultaneously administered. This value must be greater than **0**, and must be less than or equal to the value for Maximum Ports.
Maximum Concurrently Registered Remote Office Stations	Specifies the maximum number of remote office stations that are simultaneously registered, not the maximum number that are simultaneously administered. This value must be greater than **0**, and must be less than or equal to the value for Maximum Ports.
IP Stations	This value should be **y**.
Product ID	This is a 10-character field that allows any character string. For new installations, IP Soft, IP Phone, IP Agent and IP ROMax, the product IDs automatically appear
Rel. (Release)	Identifies the release number.
Limit	This field defaults to the maximum allowed value, based on the **Concurrently Registered Remote Office Stations** field on page 1 of the ***System Parameters Customer Options*** screen.

2. Type **`add station`** ***`next`*** and press **Enter** to open the **Station** screen and complete the fields listed in the table below to add a DCP station (or change an existing DCP station):

Field	Value
Type	Enter the phone model, such as **6408D**.
Port	Enter **x** if virtual, or the port number of an existing phone.

Field	Value
Security Code	Enter the user’s password.
IP Softphone	Enter **y**.

3. Go to page 2; verify whether the field **Service Link Mode:** *`as-needed`* is set as shown.
4. Install the IP Softphone software on the user’s PC.

Administering a Road-warrior phone

The sofphone application runs on a PC that is connected over an IP network. In road-warrior mode, the application uses two channels: one for call control signaling and one 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. The *init* login does not have the ability to change the customer options, offer options, or special applications screens.

To administer a Road-warrior phone:

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

   Verify that IP Softphone is enabled. Go to the appropriate pages on the **System Parameters Customer Options** screen to review the following fields:

Field	Value
Maximum Concurrently Registered IP Stations	Specifies the maximum number of IP stations that are simultaneously registered, not the maximum number that are simultaneously administered. This value must be greater than **0**.
IP Stations	Must be **y**.
Product ID	This is a 10-character field that allows any character string. For new installations, IP Soft, IP Phone, IP Agent and IP ROMax product IDs automatically display.
Rel. (Release)	Identifies the release number
Limit	Defaults to **1**

2. Type **`add station`** ***`next`*** and press **Enter** to open the **Station** screen and complete the fields listed in the table below to add a DCP station (or change an existing DCP station):

Field	Value
Type	Enter the phone model you wish to use, such as **6408D**.
Port	Enter **x** if virtual, or the port number of an existing phone. If only an IP Softphone, enter **IP**.
Security Code	Enter the user's password.
IP Softphone	Enter **y**.

3. Go to page 2; **Service Link Mode:** *`as-needed`*.

   Install the IP Softphone software on the user's PC (iClarity automatically installed with the IP Softphone R2 or greater).

Installing and administering Avaya IP telephones

The Avaya line of digital business phones 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, which enhance the administration and servicing of the phones.

For information on 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's guides.

For more information on 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 on IP Wireless Telephone Solutions, visit http://support.avaya.com

About the 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 4620SW IP telephone
- Avaya 4621SW IP telephone
- Avaya 4622SW IP telephone
- Avaya 4625 IP telephone
- Avaya 4630SW IP Screenphone

Support for SIP-enabled applications may be added to several of these IP telephones via a model-specific firmware update. See the Avaya Firmware Download Web site for more details.

About the 9600-series IP telephones

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

- Avaya 9608 IP Deskphones
- Avaya 9610 IP telephone
- Avaya 9611G IP Deskphones
- Avaya 9612G IP Deskphones
- Avaya 9620 IP telephone
- Avaya 9630 IP telephone with advanced communications capabilities

- Avaya 9640 IP telephone with advanced communications capabilities, color display
- Avaya 9641G IP Deskphones
- Avaya 9650 IP telephone

Support for SIP-enabled applications may be added to several of these IP telephones via a model-specific firmware update. See the Avaya Firmware Download Web site for more details.

About the 1600-series IP telephones

The 1600-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 1600-series IP Telephone product line includes the following telephones:

- Avaya 1603 IP telephone
- Avaya 1608 IP telephone
- Avaya 1616 IP telephone

Support for SIP-enabled applications may be added to several of these IP telephones via a model-specific firmware update. See the Avaya Firmware Download Web site for more details.

About IP telephone hardware/software requirements

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 detailed 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 Media Gateway and Avaya S8300D Server* (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`**.

Note:

Audio capability for the IP Telephones requires the presence of the TN2302AP IP Media Processor or newer packs or gateways, either of which provide hairpinning and IP-IP direct connections. Using a media processor resource conserves TDM bus and timeslot resources and improves voice quality. The voice quality is even better if the two endpoints can talk directly to each other, for example via suffling or via SIP Direct Media.

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

To install required TN2302AP, TN2602AP, and TN799DP circuit packs, if necessary

1. Determine the carrier/slot assignments of the circuit packs to be added.
2. Insert the circuit pack into the slot specified in step 1.

Note:

You do not have to power down the cabinet to install the circuit packs.

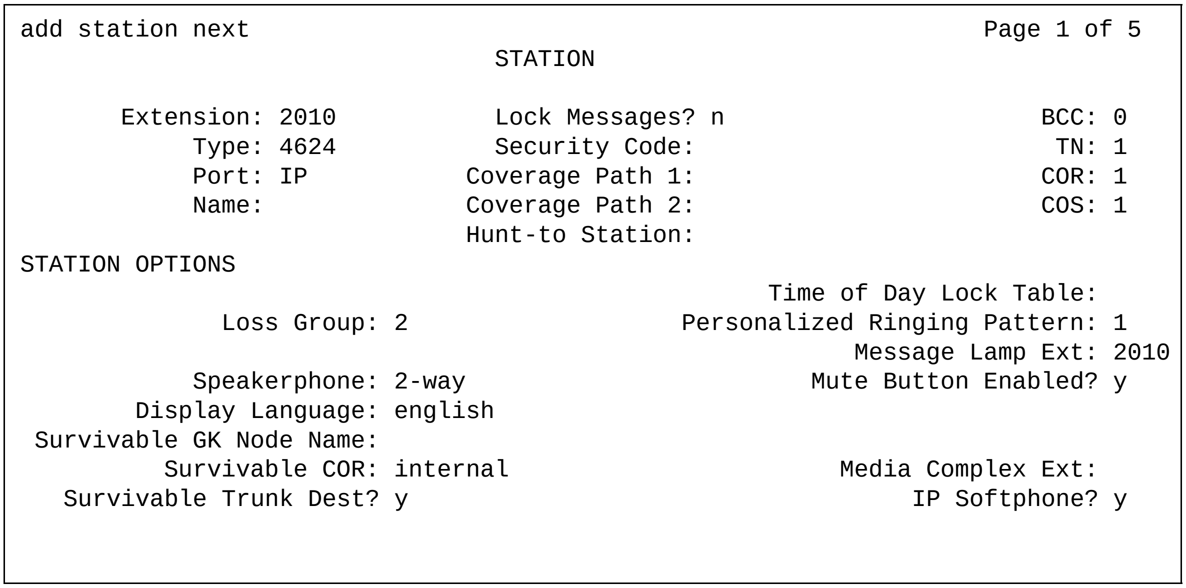
Administering Avaya IP telephones

IP Telephones R1.5 or greater use a single connection, and you only need to administer the station type.

To add an IP telephone

1. Type **`add station`** ***`next`*** to go to the **Station** screen.

Station screen



```
add station next                                                   Page 1 of 5
                                 STATION

       Extension: 2010           Lock Messages? n                         BCC: 0
            Type: 4624           Security Code:                            TN: 1
            Port: IP           Coverage Path 1:                           COR: 1
            Name:              Coverage Path 2:                           COS: 1
                               Hunt-to Station:
STATION OPTIONS
                                                    Time of Day Lock Table:
              Loss Group: 2                   Personalized Ringing Pattern: 1
                                                          Message Lamp Ext: 2010
            Speakerphone: 2-way                        Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal                       Media Complex Ext:
   Survivable Trunk Dest? y                                   IP Softphone? y
```

2. Complete the fields as shown in the following table:

Field	Value
Type	Enter 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)
Port	Enter **x**, or **IP**.

Note:

A 4600-series IP Telephone is always administered as an X port, and then once it is successfully registered by the system, a virtual port number will be assigned. (Note that a station that is registered as “unnamed” is not associated with any logical extension or administered station record.)

3. For dual-connection architecture IP Telephones (R2 or earlier), complete the fields as shown in the following table:

Field	**Value**
Media Complex Ext	Enter the H.323 administered extension.
Port	Enter **x**.

4. Submit the screen.

About hairpinning and shuffling

Communication Manager can shuffle or hairpin call path connections between two IP endpoints 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 they preserve connection and conversion resources that might not be needed, depending on the compatibility of the endpoints that are attempting to interconnect.

Shuffling and hairpinning techniques differ in the way that they bypass the unnecessary call-path resources (compare either Figure 10: Shuffled audio connection between IP endpoints in the same network region on page 92 or Figure 11: Shuffled audio connection between IP endpoints in different network regions on page 93 with Figure 12: Hairpinned audio connection between 2 IP endpoints in the same network region on page 96).

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.

Because shuffling frees up more resources on the TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit packs than hairpinning does, Communication Manager first checks both endpoints to determine whether the Determining if shuffling is possible on page 90 are met. If the shuffling criteria are not met, Communication Manager routes the call according to the What are the criteria for hairpinning on page 95, 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 on page 97. For a discussion of Network Address Translation (NAT), see About Network Address Translation on page 98.

What hardware and endpoints are required

The gateways are required for shuffling and the TN2302AP IP Media Processor,TN2602AP IP Media Resource 320 circuit pack or G700 is required for hairpinning audio connections.

The specific endpoint types that you can administer for hairpinning or shuffling are:

- All Avaya IP stations
- Other vendors' H.323-compatible stations

About shuffled audio connections

Shuffling an audio connection between two IP endpoints means rerouting voice channel away from the usual TDM bus connection and creating a direct IP-to-IP connection. Shuffling saves such resources as TN2302AP or TN2602AP channels and TDM bus time slots and improves voice quality because the shuffled connection bypasses the TN2302AP's or TN2602AP's codec. Both endpoints must be capable of shuffling (support H.245 protocol) before Communication Manager can shuffle a call.

Note:

You should preferably use SIP Direct Media over shuffling as SIP Direct Media improves the voice quality even better than shuffling. Shuffling puts the two end points together a few hundred milliseconds into the call whereas SIP Direct Media puts the two endpoints together at the very start of the call.

Determining if shuffling is possible

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 (in-use or held) that requires TDM connectivity (for example, applying tones, announcement, conferencing, and others) exists on either endpoint.
- 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 on the Station screen on page 109 or the Signaling group screen on page 107) to **y**.
- If the **Direct IP-IP Audio Connections** field is **y** (yes), but during registration the endpoint indicates that it does not support audio shuffling, then a call cannot be shuffled.

  If the **Direct IP-IP Audio Connections** field is **n** (no), but during registration the endpoint indicates that it can support audio shuffling, then calls to that endpoint cannot be shuffled, giving precedence to the endpoint administration.
- The rules for Inter-network region connection management on page 104 are met.

- There is at least one common codec 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 their 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 10: Shuffled audio connection between IP endpoints in the same network region on page 92 and Figure 11: Shuffled audio connection between IP endpoints in different network regions on page 93 provide examples of shuffled audio connections.

Figure 10: Shuffled audio connection between IP endpoints in the same network region

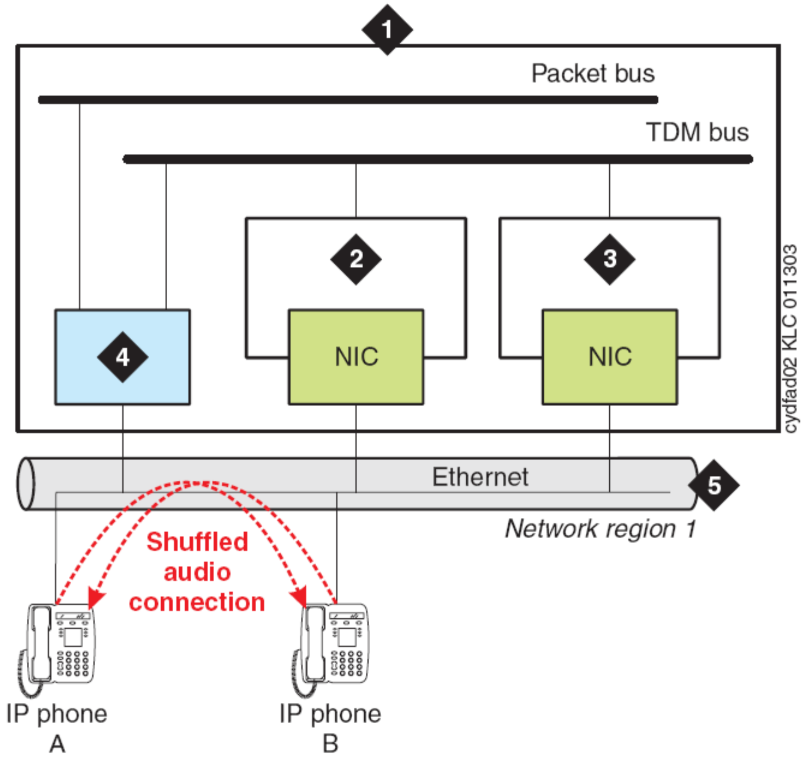


Figure notes:

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.**

Figure 10: Shuffled audio connection between IP endpoints in the same network region on page 92 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 those channels are free to serve other media connections.

Shuffling between different network regions

Figure 11: Shuffled audio connection between IP endpoints in different network regions

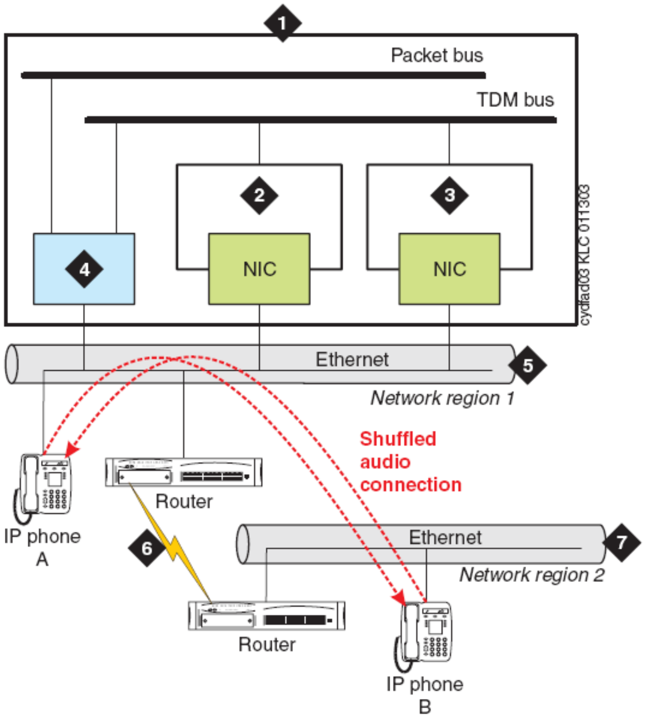


Figure notes:

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.**
6. **IP voice packet path between LAN routers**
7. **LAN/WAN segment administered in Communication Manager as network region 2.**

Figure 11: Shuffled audio connection between IP endpoints in different network regions on page 93 is a schematic of a shuffled audio connection between two IP endpoints that are in different network regions that are interconnected and the inter-network region connection management rules are met. 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.

Determining whether an endpoint supports shuffling

Placing a test call from an endpoint that is capable of shuffling to another endpoint whose shuffling capability is unknown can help you to determine whether an endpoint supports audio shuffling or not.

To determine whether an endpoint supports shuffling:

1. Administer the **Direct IP-IP Audio Connections** field on page 2 as **y** (yes) on both endpoint's station screen (**`change station`** ***`extension`***).
2. From the endpoint that can support shuffling, place a call to the endpoint that you are testing.

   Wait 2 minutes.
3. At the SAT type **`status station`** ***`extension`*** (administered extension of the endpoint that you are testing) and press **Enter** to display the **Station** screen for this extension.
4. Note the **Port** field value in the **GENERAL STATUS** section of page 1.
5. Scroll to page 4

   In the **AUDIO CHANNEL** section note the value of the **Audio** field under the **Switch Port** column.

   - If the values are the same, the endpoint is capable of shuffling.

     Administer the **Direct IP-IP Audio Connections** field (**`change station`** ***`extension`***, page 2) as **y** (yes).
   - If the values are different, then the endpoint cannot shuffle calls.

     Administer the **Direct IP-IP Audio Connections** field (**`change station`** ***`extension`***, page 2) as **n** (no).

Administrable loss plan

To prevent audio levels from changing when a 2-party call changes from the TDM bus to a shuffled or hairpinned connection, two party connections between IP endpoints are not subject to the switch's administrable loss plan. 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 of three parties or more are subject to the administrable loss plan, whether those calls involve IP endpoints or not.

About hairpinned audio connections

Hairpinning means rerouting the voice channel connecting two IP endpoints so that the voice channel goes through the TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit packs in IP format instead of through the TDM bus. Communication Manager provides only shallow hairpinning, meaning that only the IP and Real Time Protocol (RTP) packet headers are changed as the voice packets go through the TN2302AP or TN2602AP circuit pack. This requires that both endpoints use the same codec (coder/decoder), a circuit that takes a varying-voltage analog signal through a digital conversion algorithm to its digital equivalent or vice-versa (digital to analog). Throughout this section, when the word "hairpin" is used, it means shallow hairpinning.

What are the 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: the **Direct IP-IP Audio Connections** field on the Station screen on page 109 or the Signaling group screen on page 107) is **y**.
- If the **IP Audio Hairpinning** field is **y** (yes), but during registration the endpoint indicates that it does not hairpinning, then a call cannot be hairpinned.

  If the **IP Audio Hairpinning** field is **n** (no), but during registration the endpoint indicates that it can support hairpinning, then calls to that endpoint cannot be hairpinned, giving precedence to the endpoint administration.
- The Determining if shuffling is possible on page 90 are *not* met.
- 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 ms
- Preserve the Real-Time Protocol (RTP) header (for example the timestamp 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 12: Hairpinned audio connection between 2 IP endpoints in the same network region on page 96 is a schematic of a hairpinned audio connection between two IP endpoints in the same network region.

Figure 12: Hairpinned audio connection between 2 IP endpoints in the same network region

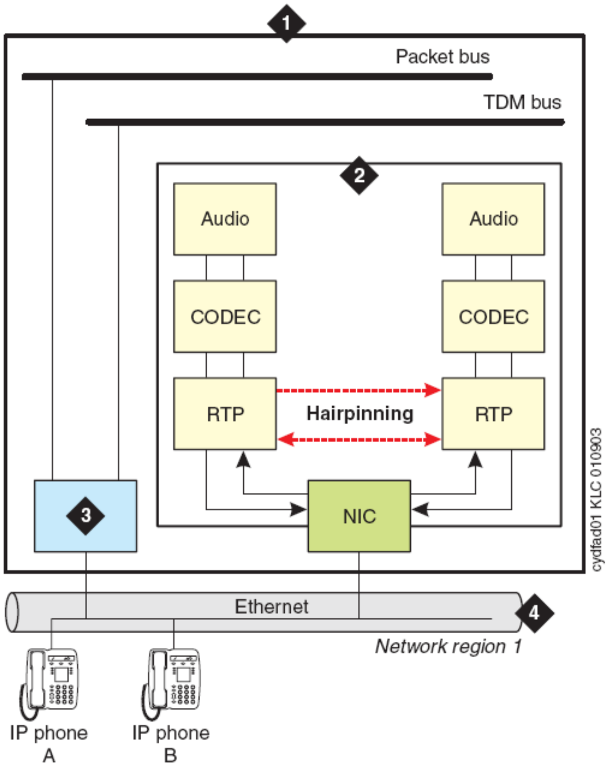


Figure notes:

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 12: Hairpinned audio connection between 2 IP endpoints in the same network region on page 96 shows that hairpinned calls bypass the TN2302AP’s or TN2602AP’s codec, thus freeing those resources for other calls. The necessary analog/digital conversions occur in the common codec in each endpoint.

What causes a hairpinned call to be redirected

Whenever a third party is conferenced into a hairpinned call or a tone or announcement must be inserted into the connection, the hairpinned connection is broken and the call is re-routed over the TDM bus.

Determining which TN2302AP or TN2602AP circuit pack is hairpinning

Whenever a TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack is hairpinning any calls, its yellow LED is on steady. Although there is no simple way to identify all of the extension numbers that are hairpinning through a particular TN2302AP or TN2602AP circuit pack, you can determine which TN2302AP or TN2602AP circuit pack a particular extension is using for hairpinning.

To determine which TN2302AP or TN2602AP circuit pack is hairpinning:

1. At the SAT, type **`status station`** ***`extension`*** and press **Enter** to display the **Station** screen for that extension.
2. Scroll to page 4 of the report.
3. In the **AUDIO CHANNEL** section, check whether there is a value in the **Audio** field under the **Switch Port** column.

   If there is no port listed, then the call is hairpinned.

Hairpinning and shuffling administration interdependencies

Table 5: Hairpinning and shuffling administration on page 98 summarizes the Communication Manager interdependencies that enable hairpinning and shuffling audio connections.

Note:

In order to use hairpinning or shuffling with either Category A or B features, the **Software Version** field (**`list configuration software-versions`**) must be **R9** or greater.

⚠ **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. This not the case for shuffling, however.

Table 5: Hairpinning and shuffling administration

Administration screen	Required customer options[1]	Other interactions
Station	IP Stations Remote Office	Hairpinning is not available if **Service Link Mode** field on ***Station*** screen is **permanent**. Shuffling is available only for the endpoints[2] Avaya IP telephone R2 and Avaya IP Softphone (R2 or newer)
Signaling group	H.323 Trunks	
Inter network region	H.323 Trunks IP Stations Remote Office	User login must have features permissions.
Feature-Related System Parameters	H.323 Trunks IP Stations Remote Office	

[1] The fields listed in this 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 of the fields listed in this column are not enabled, then either the fields for hairpinning and shuffling are not displayed or, in the case of the **Inter Network Region Connection Management** screen, the second page (the actual region-to-region connection administration) does not display.

[2] Although other vendors' fully H.323v2-compliant products should have shuffling capability, you should test that before administering such endpoints for hairpinning or shuffling. See the section titled Determining whether an endpoint supports shuffling on page 94.

About 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 and ambiguous, and they are 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 this case is the physical address, and the external address is the virtual address. This physical address does not necessarily have to be a private address as shown here, as the subscriber could pay for a public address from the broadband service provider. But regardless of the nature of the physical address, the point is that it cannot be used to communicate back to the enterprise through a VPN tunnel. Once 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.

The application of the virtual address varies among VPN clients. Some VPN clients integrate with the operating system in such a way that packets from IP applications (for example, FTP or telnet) on the enterprise host are sourced from the virtual IP address. That is, the IP applications inherently use the virtual IP address. With other VPN clients this does not occur. Instead, the 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 no different than if a router or firewall had done the translation.

What are the types of NAT

Static 1-to-1 NAT

Static 1-to-1 NAT is what has already been covered up to this point. In static 1-to-1 NAT, for every internal address there is an external address, with a static 1-to-1 mapping between internal and external addresses. It 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, and for this case there are two other types of NAT: many-to-1 and many-to-a-pool.

Dynamic Many-to-1 NAT

Dynamic many-to-1 NAT is as the name implies. 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 is known as network address port translation (NAPT) or simply port address translation (PAT). It appears to the external server that multiple requests are coming 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, allowing the external host to reply back to the internal host. It is a paradox with this type of NAT (in its simplest form) that the external host cannot generate a port mapping to initiate the communication with the internal host, and without initiating the communication, there is no way to generate the 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 general idea behind many-to-a-pool NAT is that a 1-to-1 mapping is not desired, but there are too many internal hosts to use a single external address. Therefore, a pool of multiple external addresses is used for NAT. There are enough external addresses in the pool to support all the internal hosts, but not nearly as many pool addresses as there are internal hosts.

What are the 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 is a problem that can be and has been addressed with H.323-aware NAT devices. It has also been addressed with Communication Manager 1.3 and later versions of the NAT feature.
- When an endpoint (IP telephone) registers with the gatekeeper (call server), that endpoint’s IP address must stay the same for the duration of the registration.

  This rules out almost all current implementations of many-to-a-pool NAT.
- TCP/UDP ports are involved in all aspects of IP telephony — endpoint registration, call signaling, and RTP audio transmission.

  These ports must remain unchanged for the duration of an event, duration of the registration, or duration of a call. Also, the gatekeeper must know ahead of time which ports will be used by the endpoints for audio transmission, and these ports can vary on a per call basis. These requirements make it very difficult for H.323 to work with port address translation (PAT), which rules out almost all current implementations of many-to-1 and many-to-a-pool NAT.

About the Communication Manager NAT Shuffling feature

The Communication Manager NAT Shuffling feature permits IP telephones and IP Softphones to work behind a NAT device. This feature was available prior to release 1.3, but it did not work with shuffled calls (**Direct IP-IP Audio** enabled). 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 itself (internal address)
- Translated Address — The IP address after it has gone through NAT, as seen by devices on the other side of the translation (external address)

- Gatekeeper — The Avaya device that is handling call signaling.

  It could be a portal to the gatekeeper, such as a C-LAN, or the gatekeeper itself, such as an S8300D Server.

- Gateway — The Avaya device that is handling media conversion between TDM and IP, such as a MedPro board, G700 VoIP Media Module, or any of the following Media Gateways—G450, G430, G350 or G250.

The essence of this feature is that Communication Manager keeps track of the native and translated IP addresses for every IP station (IP telephone or IP Softphone). If an IP station registration appears with different addresses in the IP header and the RAS message, the call server stores the two addresses and alerts the station that NAT has taken place.

This feature works with static 1-to-1 NAT. It 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 *may* work with many-to-a-pool NAT, if a station’s translated address remains constant for as long as the station is registered, and there is no 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 there are not two independent devices trying to compensate for H.323 at the same time.

Rules:

The following rules govern the NAT Shuffling feature. The **Direct IP-IP Audio** parameters are configured on the SAT **ip-network-region** screen.

1. When **Direct IP-IP Audio** is enabled (default) and a station with NAT and a station without NAT talk to one another, the translated address is always used.
2. When two stations with NAT talk to one another, the native addresses are used (default) when **Yes** or **Native (NAT)** is specified for **Direct IP-IP Audio**, and the translated addresses are used when **Translated (NAT)** is specified.
3. The Gatekeeper and Gateway must *not* be enabled for NAT. As long as this is true, they may be assigned to any network region.

Administering hairpinning and shuffling

Choosing how to administer hairpinning and shuffling

You can administer shuffled and hairpinned connections:

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

Table 6: Hairpinning and shuffling administration on page 102 lists the forms and provides links to all three levels:

Table 6: Hairpinning and shuffling administration

Level	Communication Manager screen	Link to procedure
System	Feature-Related System Parameters	Administering hairpinning and shuffling at the system-level on page 102
Network region	Network Region	Administering hairpinning and shuffling in network regions on page 104
IP Trunks	Signaling Group	Administering H.323 trunks for hairpinning and shuffling on page 107
IP endpoints	Station	Administering IP endpoints for hairpinning and shuffling on page 108

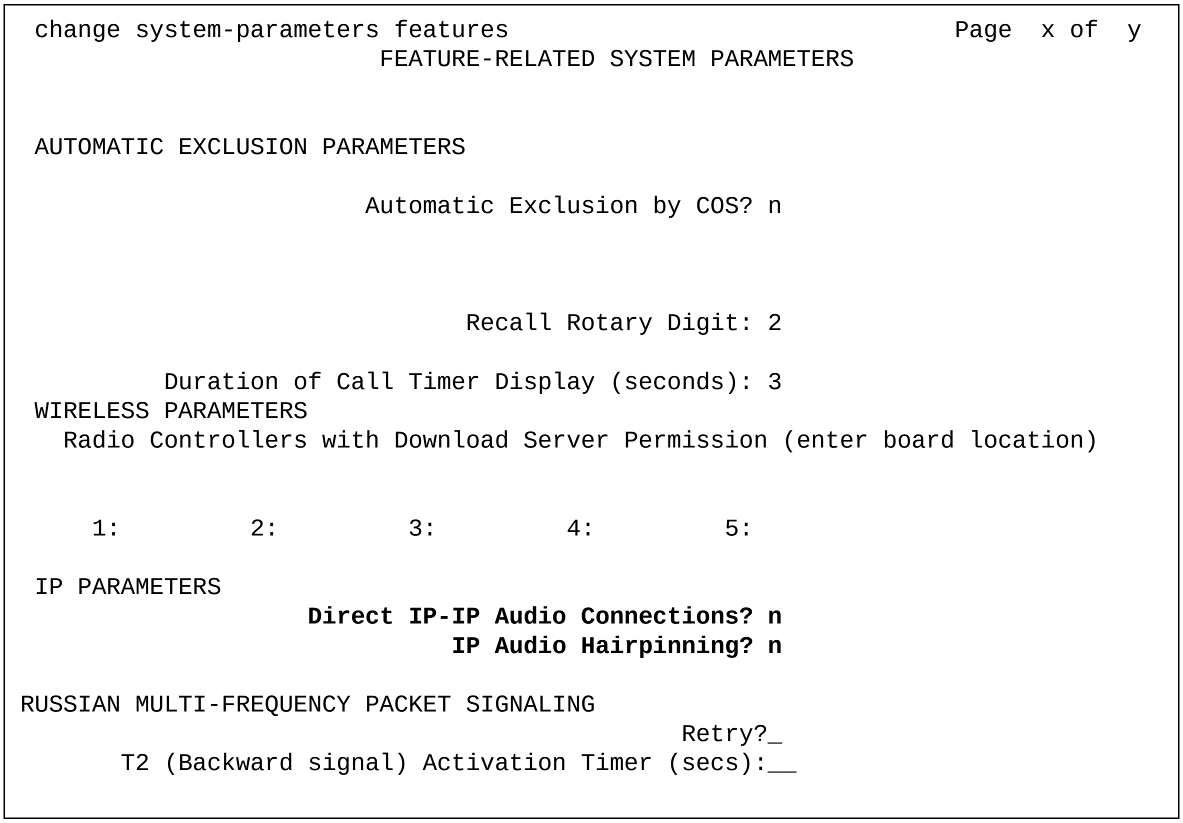
Administering hairpinning and shuffling at the system-level

You can administer hairpinning or shuffling as a system-wide parameter.

To administer hairpinning and shuffling as a system-level parameter

1. At the SAT, type **`change system-parameters features`** and press **Enter** to display the **Feature-Related System Parameters** screen:

Feature-Related System Parameters screen



```
change system-parameters features                              Page  x of  y
                        FEATURE-RELATED SYSTEM PARAMETERS


AUTOMATIC EXCLUSION PARAMETERS

                       Automatic Exclusion by COS? n



                              Recall Rotary Digit: 2

         Duration of Call Timer Display (seconds): 3
WIRELESS PARAMETERS
  Radio Controllers with Download Server Permission (enter board location)


    1:         2:         3:         4:         5:

IP PARAMETERS
                   Direct IP-IP Audio Connections? n
                             IP Audio Hairpinning? n

RUSSIAN MULTI-FREQUENCY PACKET SIGNALING
                                              Retry?_
       T2 (Backward signal) Activation Timer (secs):__
```

2. To allow shuffled IP calls using a public IP address (default), go to the page with IP PARAMETERS and set the **Direct IP-IP Audio Connections** field to **y**.

   To disallow shuffled IP calls set this field to **n**. Be sure that you understand the interactions in Hairpinning and shuffling administration interdependencies on page 97 and the notes below.

3. To allow hairpinned audio connections, type **y** (yes) in the **IP Audio Hairpinning** field, noting the interactions in Hairpinning and shuffling administration interdependencies on page 97 and the notes below.

4. Save the changes.

   Note:

   The **Direct IP-IP Audio Connections** and **IP Audio Hairpinning** fields do not display if the **IP Stations** field, the **H.323 Trunks** field, and the **Remote Office** field on the **Customer Options** screen are set to **n**.

Administering hairpinning and shuffling in network regions

Inter-network region connection management

Shuffling and hairpinning endpoints or media processing resources in any given network region is independently administered per network region, which uses a matrix to define the desired connections between pairs of regions.

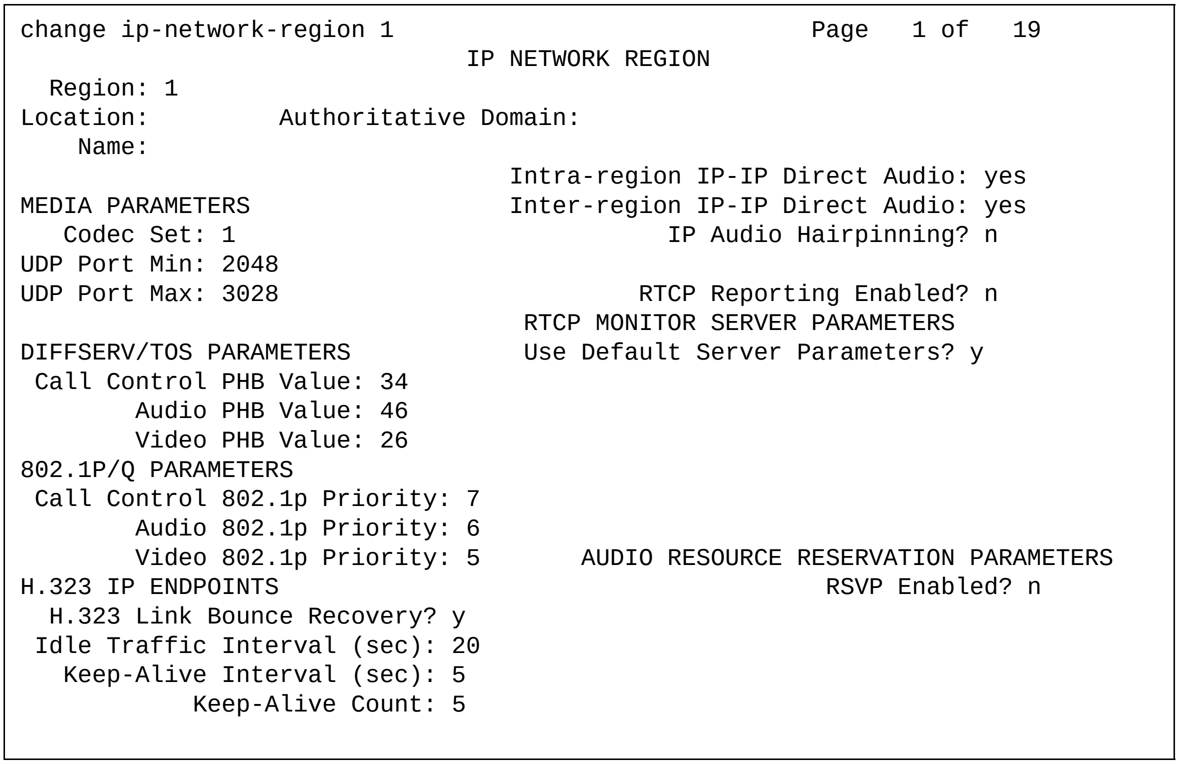
The matrix is used two ways:

- It specifies what 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 directly connected.

To administer hairpinning or shuffling within a network region:

1. At the SAT type **change `ip-network-region`** ***`number`*** and press **Enter** to display the **IP Network Region** screen.

IP Network Region screen



```
change ip-network-region 1                             Page   1 of   19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
                                  Intra-region IP-IP Direct Audio: yes
MEDIA PARAMETERS                  Inter-region IP-IP Direct Audio: yes
   Codec Set: 1                              IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3028                         RTCP Reporting Enabled? n
                                   RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS            Use Default Server Parameters? y
 Call Control PHB Value: 34
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5       AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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 allowable values for both fields are:

- **y** -- permits shuffling the call
- **n** -- disallows shuffling the call
- **native**-- the IP address of a phone itself, or no translation by a Network Address Translation (NAT) device
- **translated** -- the translated IP address that a Network Address Translation (NAT) device provides for the native address

Note:

If there is no NAT device in use at all, then the native and translated addresses are the same. For more information on NAT, see the *Administering Avaya Aura™ Communication Manager,* 03-300509 and *Avaya Application Solutions: IP Telephony Deployment Guide* (555-245-600).

3. .Go to page 3 and administer the common codec sets on the **Inter Network Region Connection Management** screen (Inter Network Region Connection Management screen on page 106). For more detailed information about the fields on this screen, see the Screen Reference chapter of the *Administering Avaya Aura™ Communication Manager,* 03-300509.

Note:

You cannot connect IP endpoints in different network regions or share TN799 C-LAN or TN2032 IP Media Processor resources between/among network regions unless you make a codec entry in this matrix specifying the codec set to be used. For more information, see Administering IP CODEC sets on page 140.

Inter Network Region Connection Management screen

```
change ip-network-region n                                        Page   3 of x

                   Inter Network Region Connection Management

 src dst codec direct    WAN-BW-limits   Video                           Dyn
 rgn rgn  set    WAN  Units     Total Norm Prio Shr Intervening-regions  CAC  IGAR
 3   1     1      y    256:Kbits
 3   2     1      n                           n  1   ___  ___  ___             n
 3   3     1
 3   4     1      n                           y  1   ___  ___  ___             n
 3   5     1      n                           y  6   ___  ___  ___
 3   6     1      y     NoLimit
 3   7     1      y     10:Calls
 3   8
 3   9     3      y
 3   10
 3   11
 3   12
 3   13
 3   14
 3   15
```

For this example screen, network region 3 communicates with:

- Network regions 1 through 7 using codec set 1
- Network region 9 using codec set 3.

Note:

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

4. Save the changes.

Administering and selecting codecs

When an IP endpoint calls another IP endpoint, Communication Manager asks that the 2nd endpoint choose the same codec that the 1st endpoint offered at call setup. However, if the 2nd endpoint cannot match the 1st's codec, the call is set up with each endpoint's administered (preferred) codec, and the data streams are converted between them, often resulting in degraded audio quality because of the different compressions/decompressions or multiple use of the same codec. For more information, see Administering IP CODEC sets on page 140.

When an endpoint (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 codec set(s) to use *within* an individual region (intra-region) and a codec set to use *between/among* (inter-region) network regions. Depending upon the network region of the requesting H.323 endpoint or trunk and the network region of the TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack:

- If the endpoint and the TN2302AP or TN2602AP are in same region, the administered intra-region codec set is chosen.

- If the endpoint and the TN2302AP or TN2602AP are in different regions, the administered inter-region codec set is chosen.

For example, a region might have its intra-network codec administered as G.711 as the first choice, followed by the other low bit rate codecs. The **Inter Network Region Connection Management** screen for the inter-network 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:

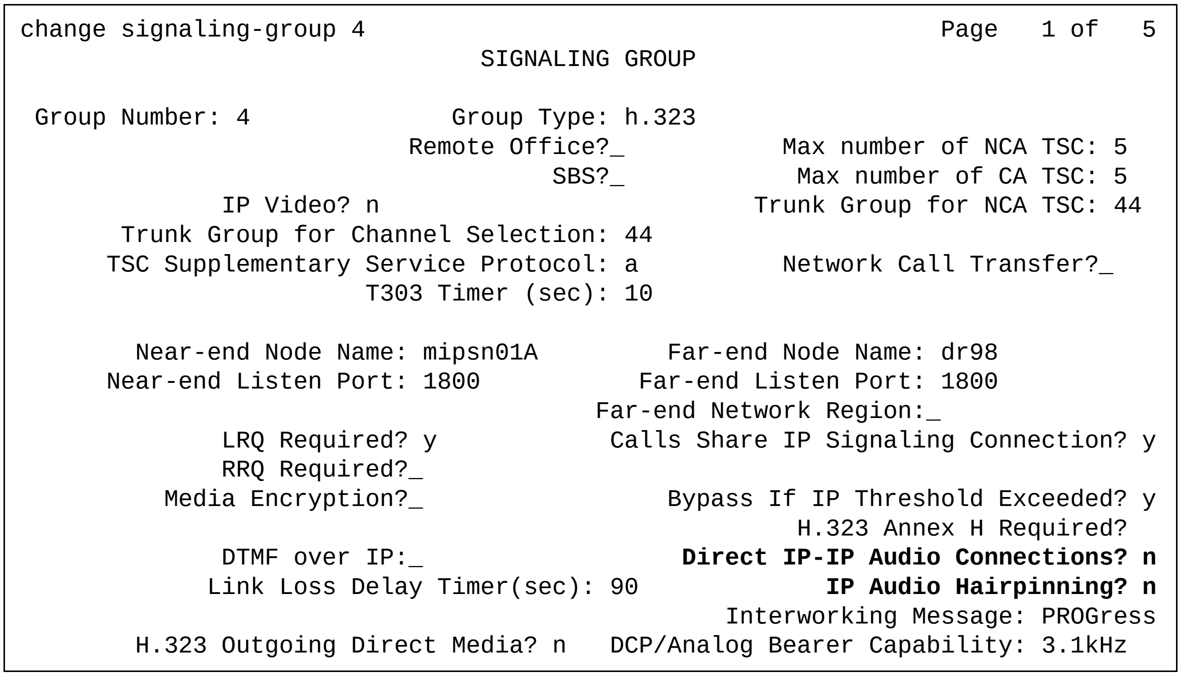
> If you are administering an H.323 trunk that uses Teletype for the Deaf (TTD), use the G.711 codec as the primary choice for those trunks. This ensures accurate TTD tone transmission through the connection.

Administering H.323 trunks for hairpinning and shuffling

To administer an H.323 trunk for hairpinning or shuffling

1. At the SAT, type **`change signaling group`** ***`number`*** and press **Enter** to display the **Signaling Group** screen (Signaling group screen on page 107).

Signaling group screen



```
change signaling-group 4                                        Page   1 of   5
                                SIGNALING GROUP

 Group Number: 4             Group Type: h.323
                          Remote Office?_            Max number of NCA TSC: 5
                                    SBS?_             Max number of CA TSC: 5
              IP Video? n                           Trunk Group for NCA TSC: 44
       Trunk Group for Channel Selection: 44
      TSC Supplementary Service Protocol: a          Network Call Transfer?_
                        T303 Timer (sec): 10

        Near-end Node Name: mipsn01A         Far-end Node Name: dr98
      Near-end Listen Port: 1800           Far-end Listen Port: 1800
                                        Far-end Network Region:_
              LRQ Required? y            Calls Share IP Signaling Connection? y
              RRQ Required?_
          Media Encryption?_                 Bypass If IP Threshold Exceeded? y
                                                      H.323 Annex H Required?
              DTMF over IP:_                  Direct IP-IP Audio Connections? n
             Link Loss Delay Timer(sec): 90             IP Audio Hairpinning? n
                                                 Interworking Message: PROGress
        H.323 Outgoing Direct Media? n   DCP/Analog Bearer Capability: 3.1kHz
```

2. To allow shuffled IP calls using a public IP address (default), set the **Direct IP-IP Audio Connections** field to **y**.

   To disallow shuffled IP calls set this field to **n**. Be sure that you understand the interactions in Hairpinning and shuffling administration interdependencies on page 97 and the notes below.

3. To allow hairpinned audio connections, type **y** (yes) in the **IP Audio Hairpinning** field, noting the interactions in Hairpinning and shuffling administration interdependencies on page 97 and the notes below.

4. Save the changes.

   Note:

   The hairpinning and shuffling fields on the **Signaling Group** screen do not display unless either the **H.323 Trunks** or **Remote Office** field is set to **y** (yes) on the **Optional Features** (**`display system-parameters customer-options`**) screen. These features must be enabled in the system's License File.

   Note:

   If you are administering an H.323 trunk that uses Teletype for the Deaf (TTD), use the G.711 codecs as the primary codec choice for those trunks to ensure accurate TTD tone transmission through the connection.

Administering IP endpoints for hairpinning and shuffling

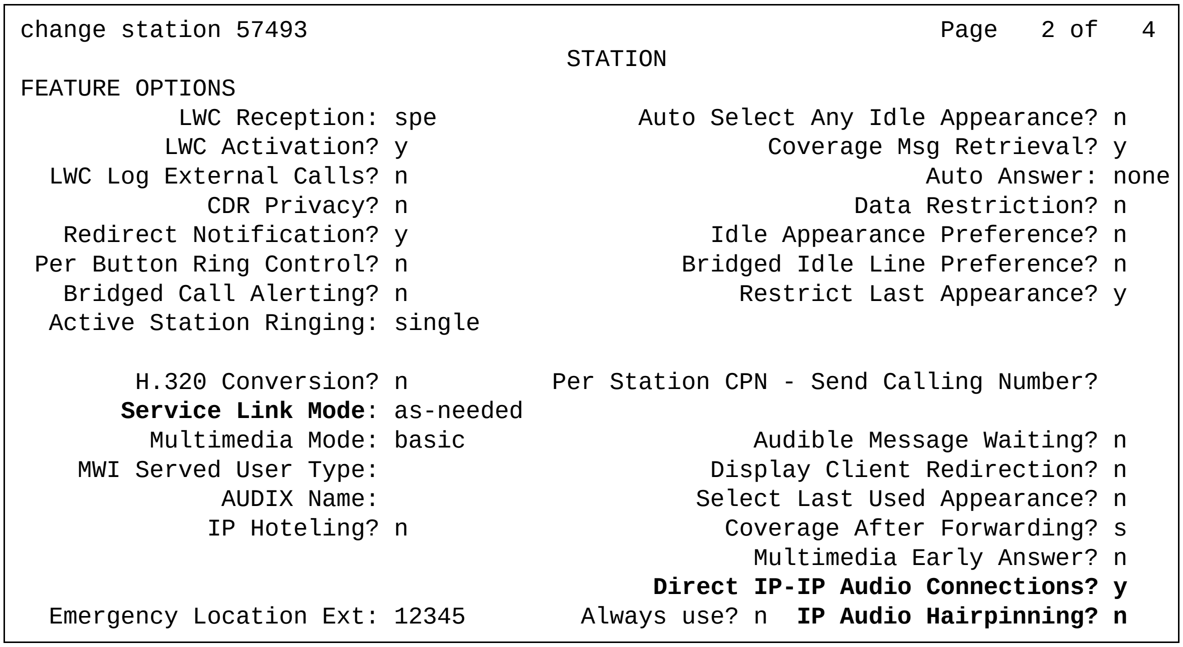
Whether any given station is allowed to shuffle or hairpin is independently administered per endpoint on the **Station** screen. The specific station types that you can administer for hairpinning or shuffling are:

- All Avaya IP stations
- Other vendors' H.323-compatible stations

To administer an IP endpoint for hairpinning or shuffling

1. At the SAT, type **`change station`** ***`extension`*** and press **Enter** to display the **Station** screen (Station screen on page 109)

Station screen



```
change station 57493                                            Page   2 of   4
                                      STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                         Coverage Msg Retrieval? y
  LWC Log External Calls? n                                    Auto Answer: none
             CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n                       Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: basic                    Audible Message Waiting? n
    MWI Served User Type:                       Display Client Redirection? n
              AUDIX Name:                      Select Last Used Appearance? n
            IP Hoteling? n                        Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
                                            Direct IP-IP Audio Connections? y
  Emergency Location Ext: 12345        Always use? n  IP Audio Hairpinning? n
```

2. To allow shuffled IP calls using a public IP address (default), set the **Direct IP-IP Audio Connections** field to **y**.

   To disallow shuffled IP calls set this field to **n**. Be sure that you understand the interactions in Hairpinning and shuffling administration interdependencies on page 97 and the notes below.

3. To allow hairpinned audio connections, type **y** in the **IP Audio Hairpinning** field, noting the interactions in Hairpinning and shuffling administration interdependencies on page 97 and the notes below.

4. Save the changes.

Note:

> The hairpinning and shuffling fields on the **Station** screen do not display unless either the **IP Stations** or **Remote Office** field is set to **y** (yes) on the **Optional Features** (**`display system-parameter customer-options`**) screen. These features must be enabled in the system's License File.

Note:

> The **Direct IP-IP Audio Connections** field cannot be set to **y** if the **Service Link Mode** field is set to **permanent**.

Contradictory IP station administration

- If an IP station is administered for dual-connect, and if the two extension numbers for that station have differing values administered in their **Direct IP-IP audio Connections** fields, then the station cannot shuffle calls.

- If an IP station is administered for dual-connect, and if the two extension numbers for that station have differing values administered in their **IP-IP Audio Hairpinning** fields, then the station cannot hairpin calls.

IP stations used for call center service-observing

If a Call Center agent is active on a shuffled call, and a Call Center supervisor wants to service-observe the call, the agent might notice the 200 ms break in the speech while the call is redirected to the TDM bus. For this reason, Avaya recommends that you administer the shuffling and hairpinning fields as **n** (no) for stations that are used for service-observing.

Administering 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 should use. The IP endpoints will always transmit audio at TIA standard levels, and expect to receive audio at TIA standard levels. If an IP audio signal goes to or comes from the TDM bus through a TN2302AP Media Processor or TN2602AP IP Media Resource 320, the circuit pack adjusts the levels to approximately equal 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.

Adjusting loss to USA DCP levels

The switch instructs the TN2302AP or TN2602AP circuit pack to insert loss into the signal coming from the IP phone, and insert gain in the signal going to the IP phone, to equal the levels of a signal to or from a DCP set.

Note:

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

Note:

The loss that is applied to a hairpinned or shuffled audio connection is constant for all three connection types: station-to-station, station-to-trunk, and trunk-to-trunk

Administering FAX, modem, TTY, and H.323 clear channel calls over IP Trunks

Communication Manager transports FAX, modem, TTY, and clear channel calls over IP interfaces using relay mode (see What is relay mode on page 111), pass-through mode (see What is pass-through mode on page 112), or both. As a result, Communication Manager supports transport of the following:

- Teletypewriter device (TTY) tone relay over the corporate IP intranet and the Internet
- Faxes over a corporate IP intranet

  Note:

  The path between endpoints for FAX transmissions must use Avaya telecommunications and networking equipment.

  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 a corporate IP intranet
- Clear channel data calls over IP

The path between endpoints for modem tone transmissions must use Avaya telecommunications and networking equipment.

What is relay mode

In relay mode, the firmware on the device (the G700/G450/G430/G350/G250 media gateway, the MM760 VoIP media module, TN2302AP Media Processor, or TN2602AP IP Media Resource 320) detects the tones of the call (FAX, modem, or TTY) and uses the appropriate modulation protocol (for FAX or modem) or Baudot transport representation (TTY) to terminate or originate the call so that it can be carried over the IP network. The modulation and demodulation for FAX and modem calls reduces bandwidth use over the IP network and improves the reliability of transmission. The correct tones are regenerated before final delivery to the endpoint.

Note:

The number of simultaneous calls that a device (gateway, media module, TN2302AP or TN2602AP) can handle is reduced by the modulation and demodulation that the device must perform for relay mode.

What is pass-through mode

In pass-through mode, the firmware on the device (the G700/G450/G430/G350/G250 media gateway, the MM760 VoIP media module, TN2302AP Media Processor, or TN2602AP IP Media Resource 320) detects the tones of the call (FAX, modem, or TTY) and uses G.711 encoding to carry the call over the IP network. pass-through mode provides higher quality transmission when endpoints in the network are all synchronized to the same clock source. The call is un-encoded before final delivery to the endpoint.

Note:

Though pass-through mode increases the bandwidth usage (per channel), it allows the same number of simultaneous FAX/modem calls on the device as the number of simultaneous voice calls. For example, on a G700 Media Gateway, pass-through allows 64 simultaneous FAX/modem calls instead of only 16 with relay.

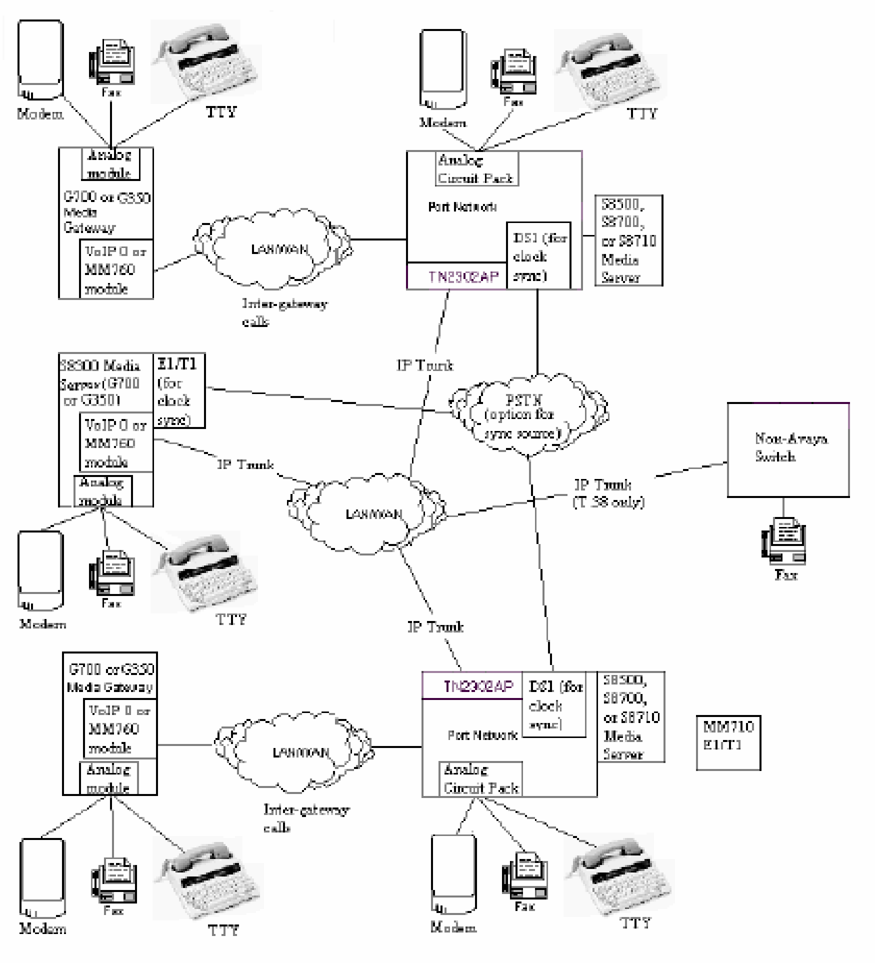
Note:

For pass-through mode on modem and TTY calls over an IP network, the sending and receiving servers should have a common synchronization source. Sychronized clocks can be established by using a source on the public network. See Figure 13: IP network connections over which FAX, modem, and TTY calls are made on page 113.

Note:

You cannot send FAXes in pass-through mode with the T.38 standard.

Figure 13: IP network connections over which FAX, modem, and TTY calls are made



Overview of steps to administer FAX, TTY, modem, and clear channel calls over IP trunks

The information in this section assumes the following:

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

To administer FAX, TTY, modem, and clear channel calls over IP trunks, first consider the following:

- FAX, TTY, modem, and clear channel transmission modes and speeds on page 115
- Considerations for administering FAX, TTY, modem, and clear channel transmission on page 119
- Bandwidth for FAX, modem, TTY, and clear channel calls over IP networks on page 122
- Media encryption for FAX, modem, TTY, and clear channel on page 123

After considering the criteria from the preceding list, complete the following tasks:

1. Create one or more IP Codec sets that enable the appropriate transmission modes for the endpoints on your gateways. See Administering IP CODEC sets on page 140.

   Note:

   You 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. See Administering IP network regions on page 147.
3. Assign the network region to the appropriate device(s):
   - TN2302AP or TN2602AP (see Defining IP interfaces (C-LAN, TN2302AP, or TN2602AP Load Balanced) on page 62)
   - Avaya G250, G350, G430, G450, or G700 Media Gateway
4. If the TN2302AP or TN2602AP resources are shared among administered network regions, administer inter-network region connections. See Figure 18: IGAR system parameter on page 166.

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

Communication Manager provides the following methods for supporting FAX, TTY, modem, and clear channel transmission over IP (see Table 7: FAX, TTY, modem, and clear channel transmission modes and speeds on page 116).

Table 7: 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 and H.323 signaling to allow communication with non-Avaya systems. The T.38 FAX capability uses the Universal Datagram Protocol (UDP). In addition, T.38 fax transmission in SIP has become a crucial feature for the messaging adjunct. Any transition from an H.323 adjunct to a SIP adjunct will have unacceptable feature debt if T.38 fax transmission is not supported over SIP. Fax support for SIP is a mainstream Advanced SIP Telephony feature that the messaging adjunct is dependant upon. **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. However, if the T.38 FAX sending and receiving endpoints are on port networks or media gateways that are registered to the same server, the gateways or port networks revert to Avaya FAX relay mode. Both the sending and receiving systems must announce support of T.38 FAX data applications during the H.245 capabilities exchange. Avaya systems announce support of T.38 FAX if the capability is administered on the Codec Set screen for the region and a T.38-capable media processor was chosen for the voice channel. In addition, for a successful FAX transmission, both systems should support the H.245 null capability exchange (shuffling) in order to avoid multiple IP hops in the connection. **Note:** To use the T.38 FAX capability, modem relay and modem pass-through must be disabled. Additionally, the T.38 FAX capability does not support TCP, FAX relay, or FAX pass-through. You can assign packet redundancy to T.38 standard faxes to improve packet delivery and robustness of FAX transport over the network.
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.

1 of 3

Table 7: FAX, TTY, modem, and clear channel transmission modes and speeds (continued)

Mode	Maximum Rate	Comments
FAX pass-through	V.34 (33.6 kbps)	The transport speed is up to the equivalent of circuit-switched calls and supports G3 and Super G3 FAX rates. ⚠ **CAUTION:** If users 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 mode, which means the media gateways use packet redundancy 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.
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 voice mode.
TTY pass-through	87-110 kbps	In pass-through mode, you can also assign packet redundancy, which means the media gateways send duplicated TTY packets to ensure and improve quality over the network. pass-through mode uses more network bandwidth than 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.

2 of 3

Table 7: FAX, TTY, modem, and clear channel transmission modes and speeds (continued)

Mode	Maximum Rate	Comments
Modem Relay	V.32 (9600 bps)	The maximum transmission rate may 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 30ms. Also, each level of packet redundancy, if selected, increases the bandwidth usage linearly (that is, 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. See your sales representative for more information. Additionally, modem relay is limited to V.32/V.32bis data rates.
Modem pass-through	V.34 (33.6 kbps) and V.90/V.92 (43.4 kbps)	Transport speed is dependent on the negotiated rate of the modem endpoints. Though the servers and media gateways support modem signaling at v.34 (33.6 bps) or v.90 and v.92 (43.4 kbps), the modem endpoints may 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 the media gateways send duplicated modem packets to improve packet delivery and robustness of FAX transport over the network. pass-through mode uses more network bandwidth than relay mode. Redundancy increases bandwidth usage even more. The maximum packet size for modem pass-through is 20 ms.
Clear Channel	64 kbps (unrestricted)	Clear channel mode supports only clear channel data. It does not support analog data transmission functionality such as FAX, modem, TTY, or DTMF signals. It is purely clear channel data. In addition, no support is available for echo cancellation, silence suppression, or conferencing. H.320 video over IP using clear channel is supported, if the port networks or the media gateways have a reliable synchronization source and transport for framing integrity.

3 of 3

Considerations for administering FAX, TTY, modem, and clear channel transmission

There are a number of factors to consider when configuring your system for FAX, TTY, modem, and clear channel calls over an IP network:

- Encryption

  You can encrypt most types of relay and pass-through calls using either the Avaya Encryption Algorithm (AEA) or the Advanced Encryption Standard (AES). See Media encryption for FAX, modem, TTY, and clear channel on page 123.

- Bandwidth usage

  Bandwidth usage of modem relay varies, depending on 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 usage 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 usage 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.

  See Table 8: Bandwidth for FAX, modem, and TTY calls over IP networks on page 122 for the bandwidth usage.

- Calls with non-Avaya systems

  For FAX calls where one of the communicating endpoints is connected to a non-Avaya communications system, the non-Avaya system and the Avaya system should both have T.38 defined for the associated codecs.

  Modem and TTY calls over the IP network *cannot* be successfully sent to non-Avaya systems.

- Differing transmission methods at the sending/receiving endpoints

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

  In some cases, a call succeeds even though the transmission method for the sending and receiving endpoints is different. Generally, however, 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, if the Port Networks or the Media Gateways involved have reliable individual Synchronization Sources and transport for framing integrity of the channels.

- Hardware requirements

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

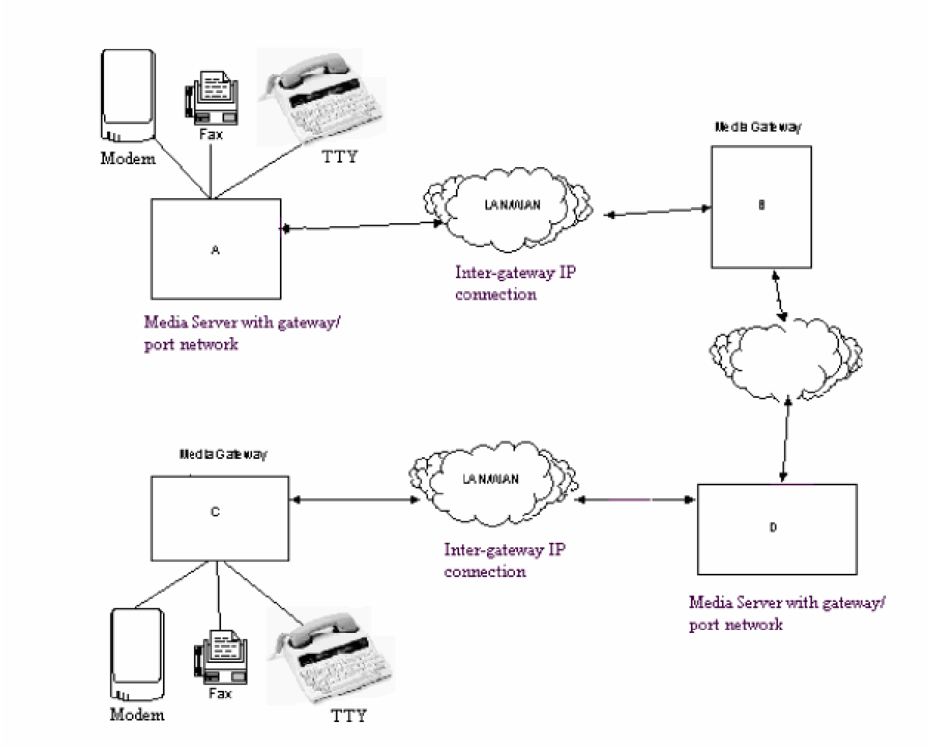
  - For Simplex and Duplex servers, certain minimum hardware vintages and firmware versions are required for the TN2302AP or the TN2602AP circuit pack; see the document titled *Avaya Aura™ Communication Manager Minimum Firmware/Hardware Vintages* at http://www.avaya.com/support.
  - For the G700 and G350 Media Gateways, the respective firmware version 22.14.0, and VoIP firmware Vintage 40 or greater to support Communication Manager 2.2 is required. An MM760 Media Module with firmware Vintage 40 or greater may be used for additional VoIP capacity. Check the latest firmware on the http://www.avaya.com/support website.
  - For the Avaya S8300D Servers, the Avaya G250 Media Gateway, and the Multi-Tech MultiVoIP Gateway, the firmware should be updated to the latest available on the http://www.avaya.com/support website.
  - For T.38 FAX capability, endpoints on other non-Avaya T.38 compliant communications systems may send FAX calls to or receive FAX calls from endpoints on Avaya systems.

- Multiple hops and multiple conversions

  If a FAX call must undergo more than one conversion cycle (from TDM protocol to IP protocol and back to TDM protocol), FAX pass-through should be used. If FAX relay mode is used, the call may fail due to delays in processing through more than one conversion cycle. A modem or TTY call may undergo no more than one conversion cycle (from TDM protocol to IP protocol and back to TDM protocol) on the communication path. If multiple conversion cycles occur, the call fails. As a result, 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 Figure 14: Shuffling for FAX, modem, and TTY calls over IP on page 121, a hop occurs in either direction for calls between port network A and Media Gateway C because the calls are routed through port network D. In this case, shuffling is required on port network A for calls going to Media Gateway C, and shuffling is required on port network D for calls going from Media Gateway C to port network A.

Figure 14: Shuffling for FAX, modem, and TTY calls over IP



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 packet sizes used, redundancy used, and whether the relay or pass-through method is used.

Table 8: Bandwidth for FAX, modem, and TTY calls over IP networks

Packet Size (in msec	Bandwidth (in kbps) (bidirectional)[1]									
	Redundancy = 0						Redundancy = 1		Red. = 2	Red. = 3
	TTY at G.711	TTY at G.729	TTY at G.723[2]	FAX Relay[3]	Modem Relay at 9600 Baud[4]	Clear Channel FAX/Modem pass-through[5] [6]	FAX Relay[3] [4]	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	-	-	-	-	-

1. TTY, Modem Relay, Modem pass-through and FAX pass-through calls are full duplex. Multiply the mode's bandwidth by 2 to get the network bandwidth usage.
2. TTY at G723 supports packet size 30 and 60 ms.
3. FAX Relay supports packet size 30ms.
4. Non-zero redundancy options increase the bandwidth usage by a linear factor of the bandwidth usage when the redundancy is zero.
5. FAX and Modem pass-through supports packet sizes 10 and 20 ms.
6. 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 will be 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 non-encrypted calls.

Encryption is applicable as shown in the following table.

Table 9: Encryption options

Call Type	AEA	AES	SRTP[1]	Transport
Modem Pass-through	Y	Y	Y	RTP (RFC2198)
Modem Relay	Y	N	N	Proprietary
FAX Pass-through	Y	Y	Y	RTP
FAX Relay	Y	(Y)[2]	N	Duplicate Packets
TTY Pass-through	Y	Y	Y	RTP
TTY Relay	Y	Y	Y	RTP
T.38 FAX Standard	(Y)[3]	(Y)[3]	N	T.38 UDPTL Redundancy
Clear Channel	Y	Y	Y	Clear 64 kbps over RTP

[1] See SRTP media encryption on page 124 for a description of the SRTP encryption protocol.

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

[3] 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 for the call's duration.

The software behaves in the following way for encryption:

1. For FAX, modem, and TTY pass-through and relay, the 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.

2. For T.38 FAX, the VoIP firmware encrypts the voice channel as administered on the codec set screen. When the call is converted to FAX, the VoIP firmware automatically turns off encryption. If the call later reverts back to audio, VoIP firmware encrypts the stream again.

SRTP media encryption

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

Following is the backward compatibility analysis with SDP cap-neg support:

1. Communication Manager(with SDP cap-neg support) when performing SIP signalling with CM4.0/ADO 1.2/SPARK 1.2(existing SRTP support), the calls will result in RTP where SRTP and non encryption choices are allowed at both sides. With current SRTP implementation, such calls result in SRTP.
2. SIP Endpoints(with SDP cap-neg support) when performing SIP signalling with CM4.0/ADO 1.2/SPARK 1.2(existing SRTP support), the calls will result in RTP where SRTP and non encryption choices are allowed at both sides. With current SRTP implementation, such calls result in SRTP.
3. SIP UA(with SDP cap-neg support) with(SRTP,none) policy when performing SIP signalling with SIP UA(with existing SRTP support) with (SRTP only) policy, the calls WILL FAIL.

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

- Encryption of RTP (optional but recommended)
- Authentication of RTCP streams (mandatory)
- Authentication of RTP streams (optional but recommended)
- Protection against replay

The following SRTP features are currently not supported by Communication Manager:

- Encryption of RTCP streams
- Several automatic rekeying schemes
- Various other options within SRTP which 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 but no media encryption was available for SIP calls. Starting with release 4.0, SRTP provides encryption and authentication of RTP streams for SIP and 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 because they are not transmitted in RTP. For this reason, in the case where an SRTP voice call changes to fax relay, fax will not be encrypted.

SRTP is available only if Media Encryption is enabled in the license file and is activated by IP codec set administration in the same manner as for the other encryption algorithms.

Platforms

The SRTP feature is supported on all Linux-based platforms running Communication Manager.

The following gateway platforms also support SRTP:

- TN2602AP Media Resource 320
- MM760
- VoIP Media Modules and on-board VoIP engines (IG550,G700,G430, G450,G350 and G250).

Administering SRTP

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

1. Ensure that media encryption is enabled. The Media Encryption? field must be set to ***y*** on the Customer Options form.
2. Administer the Media Encryption type on the ip-codec-set form:

   Media Encryption field — This field appears only if the **Media Encryption over IP** feature is enabled in the license file. Use this field to specify a priority listing of the three possible options for the negotiation of encryption.
3. Administer the ip-network-region form for SIP options:

   Allow SIP URI Conversion? field — Use this 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 would be less secure but this may be necessary to complete the call. If you enter **n** for 'no' URI conversion, then calls made from SIP endpoints that support SRTP to other SIP endpoints that do not support SRTP will fail. Enter **y** to allow conversion of SIP URIs. The default is **y**.
4. You must configure an endpoint (telephone) 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 "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)

See About Media Encryption on page 177 for more information about administering SRTP.

Chapter 5: Voice and Network quality administration

This chapter provides information about:

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

The topics covered are:

About factors causing voice degradation introduces the types of voice degradation and their causes.

About Quality of Service (QoS) and voice quality administration tells you how to administer your Avaya equipment for better voice quality and offers suggestions for other network problems.

About Media Encryption discusses media encryption capabilities, requirements, and administration in Communication Manager.

Network recovery and survivability includes information about administering H.248 Link Recovery and the Avaya Policy Manager (APM) and Avaya VoIP Monitoring Manager network monitoring tools.

Note:
Implementing QoS requires administration adjustments to Avaya equipment as well as LAN/WAN equipment (switches, routers, hubs, etc.).

For more information about QoS in Avaya IP Telephony networks, see *Avaya Application Solutions: IP Telephony Deployment Guide*, 555-245-600.

For more information on implementing QoS, see the White Paper, *Avaya IP Voice Quality Network Requirements (LB1500-02)*, at http://support.avaya.com/css/P8/documents/100018203.

About factors causing voice degradation

VoIP applications put severe constraints on the amount of end-to-end transfer delay of the 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 of the general complaints and their causes are listed in Table 10: User complaints and their causes on page 128.

Table 10: User complaints and their causes ***1 of 2***

Complaint	**Possible causes and links to information**
'Talking over' the far end	● Packet delay and loss ● Echo ● Network architecture between endpoint and intermediate node ● Switching algorithms
Near-end or far-end hear(s) echo	● Impedance mismatch ● Improper coupling ● Codec administration
Voice is too soft or too loud	● PSTN loss ● Digital loss ● Automatic Gain Control ● Conference loss plan
	1 of 2

Table 10: User complaints and their causes ***2 of 2***

Complaint	Possible causes and links to information
Clicks, pops, or stutters	● Packet loss ● Timing drift due to clocks ● Jitter ● False DTMF detection ● Silence supprSurvivable Core serverion algorithms
Voice sounds muffled, distorted, or noisy	● Codec administration ● Transducers ● Housings ● Environment ● Analog design
	2 of 2

Some of the factors causing voice degradation are:

- Packet delay and loss
- Echo
- Transcoding

Packet delay and loss

The causes of voice degradation include:

- Packet delay (latency)
  - Buffer delays
  - Queuing delays in switches and routers
  - Bandwidth restrictions
- Jitter (statistical average variance in end-to-end packet travel times)
- Packet loss
  - Network overloaded
  - Jitter buffers filled
  - Echo

For a detailed discussion of packet delay and loss, see the section on "Voice quality network requirements" in *Avaya Application Solutions: IP Telephony Deployment Guide* (555-245-600).

Tip:
Avaya recommends a network assessment that measures and solves latency issues before implementing VoIP solutions. For more information, see *Avaya Application Solutions: IP Telephony Deployment Guide* (555-245-600).

Echo

When you hear your own voice reflected back with a slight delay, this is echo and it happens for the following reasons:

- Electrical -- from unbalanced impedances or cross-talk
- Acoustical -- introduced by speakerphone or room size

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

Note:
VoIP itself is not a cause of echo. However, significant amounts of delay or jitter associated with VoIP can make echo perceptible that would otherwise not be perceived.

Echo cancellers

Echo cancellers minimize echo by comparing the original voice pattern with the received pattern, and cancelling the echo if the patterns match. However echo cancellers are not perfect, when,

- The round-trip delay from the echo canceller to the echo reflection point and back is longer than the time that the original (non-echoed) signal is buffered in the echo canceller memory. The larger the echo canceller’s memory , the longer the signal is held in the buffer, maximizing the number of packets that the canceller can compare in the allotted time.
- 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 3dB greater indicates far-end speech.

Echo cancellers do not work well over analog trunks and with speakerphones with volume controls that permit strong signals. Although VADs can greatly conserve bandwidth, more aggressive VADs can cause voice clipping and reduce voice quality. VAD administration is done on the **station** screen for the particular IP phone.

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

Echo cancellation configurations (TN464HP/TN2464CP circuit packs)

The following summarizes the echo cancellation configurationss that are available exclusively for the TN464HP/TN2464CP circuit packs. For echo cancellation configurations that are available for the TN464GP/TN2464BP circuit packs, see Echo cancellation configurations (TN464GP/TN2464BP circuit packs) on page 132.

Echo Cancellation Configuration 1 - TN464HP/TN2464CP

This plan is recommended. It has comfort noise generation and residual echo suppression turned on. During "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 assumed chosen to cancel the talker’s echo. Since this plan turns on comfort noise and echo suppression, it is similar to EC plans 8 and 9 for the TN464GP/TN2464BP circuit packs.

Echo Cancellation Configuration 2 - TN464HP/TN2464CP

This configuration has comfort noise generation turned off and residual echo suppression turned on. This plan works well in a quiet background environment. In a noisy background environment, background noise pumping or clipping is heard by the talker. In this case, EC direction is assumed chosen to cancel the talker's echo. This plan may be a good compromise for a small percent of users, who do not care for the comfort noise and prefer the silence during the residual echo suppression periods. Since the plan turns off comfort noise and turns on residual suppression, it is similar to EC configurations 1-6 for the TN464GP/TN2464BP circuit packs.

Echo Cancellation Configuration 3 - TN464HP/TN2464CP

This configuration 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's preferences. Situations that require configuration 3 should be very rare. (For example, the user does not care for the sound of comfort noise nor the pumping or clipping of background noise.) This configuration allows the user to hear sound from the earpiece as natural as possible. However, the user may hear residual echo during training periods, or all the time if echo is sufficiently high and residual echo is always present. Convergence may be very slow. Since comfort noise and residual suppression are turned off, this configuration is similar to EC configuration 7 for the TN464GP/TN2464BP circuit packs.

Echo cancellation configurations (TN464GP/TN2464BP circuit packs)

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

Note:
An EC configuration setting can be changed in real time.The change takes effect immediately. That is, it is not necessary to busyout/release the circuit pack – you simply change the setting on the **DS1 Circuit Pack** screen. This can be done without disruption to existing calls - in fact, you immediately hear the effect of the change.

⚠ **Important:**
When there are TN2302AP or TN2602AP circuit pack(s) and TN464GP/TN2464BP circuit pack(s) being used for a call, the echo canceller on the TN2302AP or TN2602AP is turned off and the echo canceller on the TN464GP/TN2454BP is used instead, because it has the greater echo canceller.

The following summarizes the echo cancellation configurations that are available for the TN464GP/TN2464BP circuit packs. For echo cancellation configurations that are available exclusively for the TN464HP/TN2464CP circuit packs, see Echo cancellation configurations (TN464HP/TN2464CP circuit packs) on page 131.

Echo Cancellation Configuration 1 – Highly Aggressive Echo Control

This configuration can control very strong echo from a distant party. It (as well as Echo Cancellation Configuration 4) provides the most rapid convergence in detecting and correcting echo at the beginning of a call. The initial echo fades faster than the other settings (generally in a small fraction of a second), regardless of the loudness of the talker's voice. 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. This makes EC Configuration 1 a good choice for consistently high network signal levels. EC Configuration 1 can cause low-volume complaints and/or complaints of clipped speech utterances, particularly when both parties speak simultaneously (doubletalk). Because EC Configuration 1 relies strongly on echo suppression to help control echo, "pumping" of the distant party's background noise may occur and lead to complaints. Prior to Communication Manager Release 2.0, EC Configuration 1 was the default configuration.

The 6dB of loss in EC Configuration 1 is in one direction only and 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 additional 6dB of signal loss, *and* convergence of the echo canceller is slower, but more stable than that provided by EC Configuration 1. If EC Configuration 1 is found to diverge during doubletalk conditions – noticeable by the sudden onset of audible echo, EC Configuration 2 should be used in place of EC Configuration 1. Because the echo canceller converges somewhat slower, some initial echo may be noticeable at the start 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 strongly on echo suppression to help control echo, "pumping" of the distant party's background noise may 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 even more stable. Because the echo canceller converges somewhat slower, some initial echo may 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 strongly on echo suppression to help control echo, "pumping" of the distant party's background noise may occur and lead to complaints.

Echo Cancellation Configuration 4 – Highly Aggressive Echo Control

Echo Cancellation Configuration 4 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 strongly relies on echo suppression to help control echo, “pumping” of the distant party’s background noise may occur, and lead to complaints.

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

Echo Cancellation Configuration 5 departs significantly from EC Configurations 1 –4. The echo canceller is slower to converge and is very stable once it converges. Some initial echo may be heard at the beginning of a call. EC Configuration 5 will not, in general, lead to complaints of clipped speech or pumping of the distant party’s background noise.

Echo Cancellation Configuration 6 – Highly Aggressive Echo Control

Echo Cancellation Configuration 6 is identical to EC Configuration 4, but reliance on the echo suppressor to control echo is about one-half that of EC Configuration 4. As a result, EC Configuration 6 will not clip speech as much as EC Configuration 4, but may cause somewhat more audible echo, particularly at the start of a call. Some pumping of the distant party’s background noise may be perceptible.

Echo Cancellation Configuration 7 – Extremely Moderate & Stable Echo Control

Echo Cancellation Configuration 7 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 may linger for several seconds as the echo canceller converges.

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

Echo Cancellation Configuration 8 provides aggressive control of echo at the start of a call and more moderate control during the call. Unlike all prior settings, EC Configuration 8 uses “comfort noise” injection to match the actual noise level of the distant party’s speech signal. The effect is one of echo canceller “transparency,” in which complaints of clipped speech or noise pumping should be few to none. To many people, EC Configuration 8 and EC Configuration 9 will be indistinguishable.

Echo Cancellation Configuration 9 – Aggressive, Transparent Echo Control 2

Echo Cancellation Configuration 9 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 will be indistinguishable.

Transcoding

When IP endpoints are connected through more than one network region, it is important that each region use the same CODEC, the circuitry that converts an audio signal into its digital equivalent and assigns its 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 (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 there may be no data in the network.

While most data applications are insensitive to small delays, the recovery of lost and corrupted voice packets poses a significant problem. For example, users might not really be concerned if the reception of E-mail 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 this the network resources are required for the complete duration of the call. If in any instance, there are no resources or the network too busy to carry the voice packets, then the destination experiences clicks, pops and stutters. Therefore, there is a continuous need for a fixed amount of bandwidth during the call to keep it real-time and clear.

About Quality of Service (QoS) and voice quality administration

Of the VoIP network issues described in the About factors causing voice degradation section, delay is the most crucial. And because many of the other causes are highly interdependent with delay, the primary goal is to reduce delay by improving the routing in the network, or by reducing the processing time within the end points and the 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, and packets will not be 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 due to network congestion or queuing can be minimized by adjusting these 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 Administering IP network regions on page 147).

Layer 3 QoS

DiffServ

The Differentiated Services Code Point (DSCP) or “DiffServ” is a packet prioritization scheme that uses the Type of Service (ToS) byte in the packet header to indicate the packet’s forwarding class and Per Hop Behaviors (PHBs). After the packets are marked with their 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, and 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 amount 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 their forwarding class, the interior nodes (routers & gateways) can use this information to differentiate the 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 transmits requests for resource reservations to routers on the path between the sender and the receiver for the voice bearer packets only, not the call setup or call signaling packets.

Layer 2 QoS: 802.1p/Q

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

⚠ **CAUTION:**
If you change 802.1p/Q on the IP Network Region screen, it changes the format of the Ethernet frames. 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 since PC-based endpoints must prioritize audio traffic over routine data traffic.

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

802.1p/Q provides for 8 priority levels and for a large number of 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 individual links. 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 ignore the VLAN on/off options, because turning VLAN on requires that the capabilities be administered on the closet LAN switch nearest 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. This requires a separate network region for each network interface.

Using 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 the nodes that are members of this VLAN. This reduces CPU utilization and increases security by restricting the traffic to a few nodes rather than every node on the LAN.

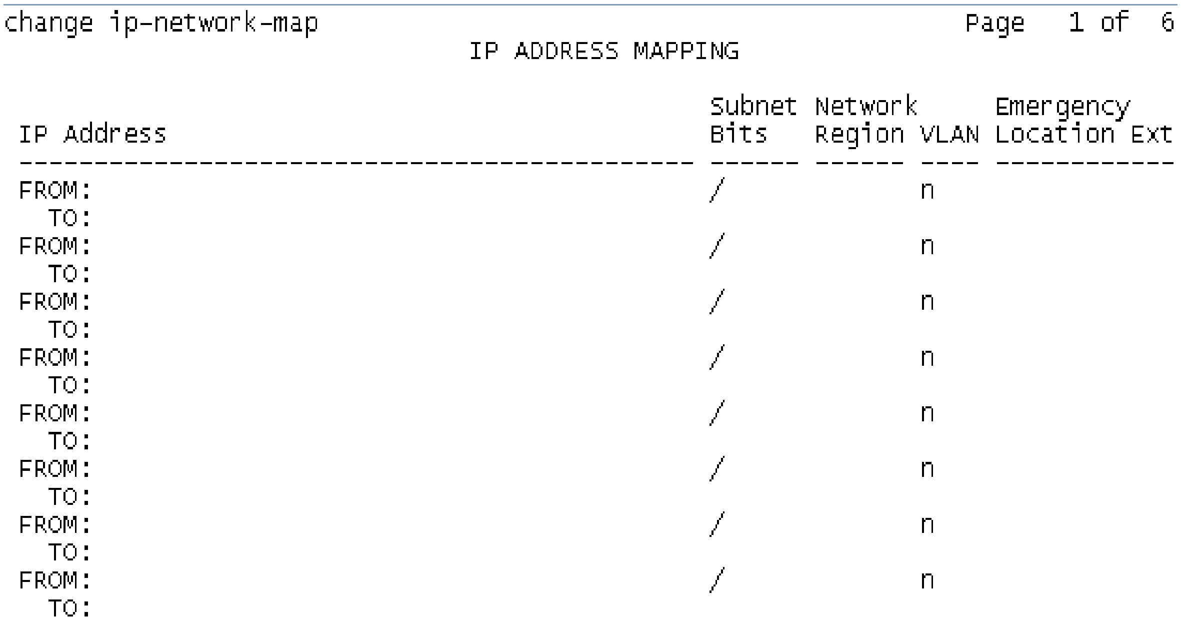
Any end-system that performs VLAN functions and protocols is “VLAN-aware,” although currently very few end-systems are VLAN-aware. VLAN-unaware switches cannot handle VLAN packets (from VLAN-aware switches), and this is why Avaya’s gateways have VLAN configuration turned off by default.

Avaya strongly recommends creating 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) on page 62)
- Endpoint-level administration on the **IP Address Mapping** screen

To administer endpoints for IP address mapping

1. Type **`change ip-network-map`** and press **Enter** to display the IP Address Mapping screen.



```
change ip-network-map                                            Page   1 of   6
                          IP ADDRESS MAPPING

                                                     Subnet  Network     Emergency
 IP Address                                          Bits    Region VLAN Location Ext
 --------------------------------------------------- ------  ------ ---- ------------
 FROM:                                               /              n
   TO:
 FROM:                                               /              n
   TO:
 FROM:                                               /              n
   TO:
 FROM:                                               /              n
   TO:
 FROM:                                               /              n
   TO:
 FROM:                                               /              n
   TO:
 FROM:                                               /              n
   TO:
 FROM:                                               /              n
   TO:
```

2. Complete the following fields:

Table 11: IP Address Mapping screen fields

Field	**Conditions/Comments**
FROM IP Address	Defines the starting IP address. A 32-bit address (four decimal numbers, each in the range **0-255**).
TO IP Address	Defines the termination of the IP address. If this field and the **Subnet Mask** field are blank when submitted, the address in the **From IP Address** field is copied into this field. A 32-bit address (four decimal numbers, each in the range **0-255**).
or Subnet Mask	Specifies the mask to be used to obtain the subnet work identifier from the IP address. If this field is non-blank on submission, then: ● Mask applied to **From IP Address** field, placing zeros in the non-masked rightmost bits. This becomes the stored "From" address. ● Mask applied to **To IP Address** field, placing 1’s in the non-masked rightmost bits. This becomes the stored "To" address. If this field and the **To IP Address** field are blank when submitted, the address in the **From IP Address** field is copied into the **To IP Address** field. Valid entries: **0-32**, or blank.
Region	Identifies the network region for the IP address range. Valid entries: **1-250** (Enter the network region number for this interface.)
VLAN	Sends VLAN instructions to IP endpoints such as IP telephones/IP Softphones. This field does not send instructions to the PROCR, C-LAN, or Media Processor boards. Valid entries: **0-4095** (specifies the virtual LAN value); **n** (disabled).

3. Submit the screen.

Administering IP CODEC sets

The **IP Codec Set** screen allows you to specify the type of CODEC used for voice encoding and companding, and compression/decompression. 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.

The **IP Codec Set** screen allows you to 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 10ms-frames you administer per packet.

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

- Whether or not endpoints in the assigned network region can route FAX, modem, TTY, or clear channel calls over IP trunks
- Which mode the system uses to route the FAX, modem, TTY, or clear channel calls
- Whether or not redundant packets will 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 for endpoints in that region to be able to use the capabilities established on this screen.

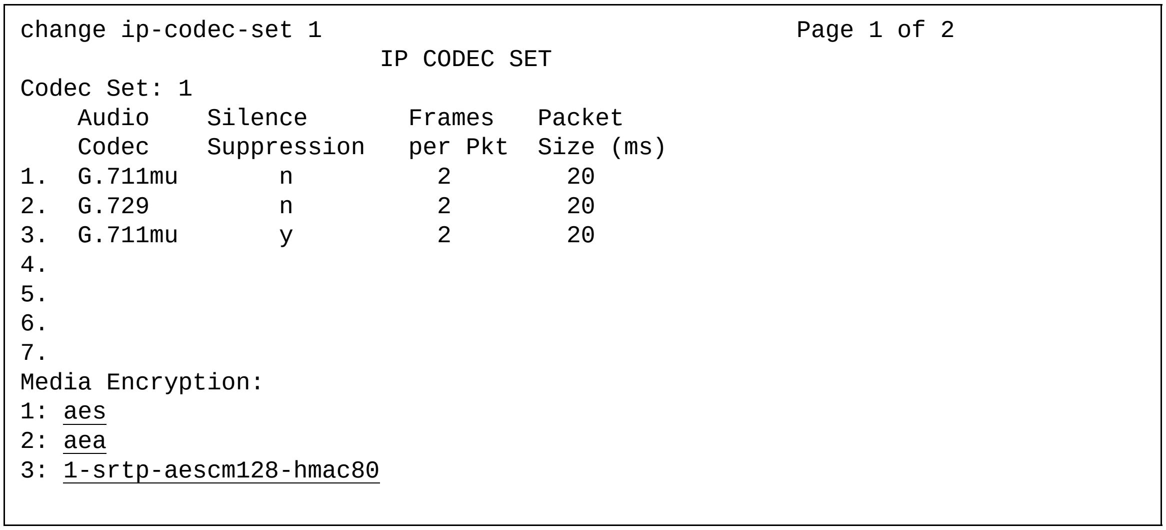
CAUTION:
If users are using Super G3 FAX machines as well as modems, do *not* assign these FAX machines to a network region with an IP Codec set that is modem-enabled as well as FAX-enabled. If its Codec set is enabled for both modem and FAX signaling, a Super G3 FAX machine incorrectly tries to use 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.

To administer an IP Codec set

1. Type **change `ip-codec-set` *`set#`*** and press **Enter** to open the **IP Codec Set** screen.

IP Codec Set screen, Page 1



```
change ip-codec-set 1                                             Page 1 of 2
                         IP CODEC SET
Codec Set: 1
    Audio    Silence       Frames   Packet
    Codec    Suppression   per Pkt  Size (ms)
1.  G.711mu       n          2        20
2.  G.729         n          2        20
3.  G.711mu       y          2        20
4.
5.
6.
7.
Media Encryption:
1: aes
2: aea
3: 1-srtp-aescm128-hmac80
```

2. Complete the fields in .Figure 12

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:

- G.711 A-law — 85 kbps
- G.711 mu-law — 85 kbps (used in U.S. and Japan)
- G.729 — 30 kbps
- G.729A/B/AB — 30 kbps audio

Table 12: IP Codec Set screen fields, page 1

Field	Conditions/Comments
Audio Codec	Specifies an audio CODEC. Valid values are: ● **G.711A** (a-law) ● **G.711MU** (mu-law) ● **G.722- 64k** ● **G.722.1- 24k** ● **G.722.1- 32k** ● **G.723- 5.3k** ● **G.723- 6.3k** ● **G.726A- 32k** ● **G.729** ● **G.729A** ● **G.729B** ● **G.729AB** ● **SIREN14- 24k** ● **SIREN14- 32k** ● **SIREN14- 48k** ● **SIREN14- S48k** ● **SIREN14- S56k** ● **SIREN14- S64k** ● **SIREN14- S96k**
Silence Suppression	Enter **n** (recommended). Enter **y** if you require silence suppression on the audio stream. This may affect audio quality.
Frames per Pkt	Specifies frames per packet. Enter a value between **1-6**. Default values are: ● **2** for G.711 Codec (frame size 10ms) ● **2** for G729 Codec (frame size 10ms)
Packet Size (ms)	Automatically appears.
	1 of 2

Table 12: IP Codec Set screen fields, page 1 (continued)

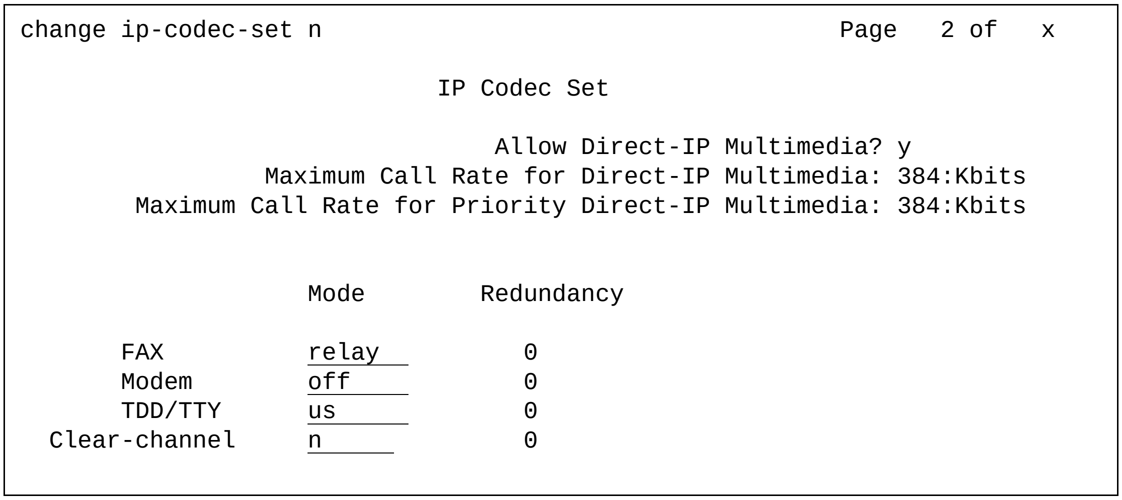
Field	Conditions/Comments
Media Encryption	This field appears only if the **Media Encryption over IP** feature is enabled. It specifies one of three possible options for the negotiation of encryption. The selected option for an IP codec set applies to all codecs defined in that set. Valid entries are: ● **aes** — Advanced Encryption Standard (AES), a standard cryptographic algorithm for use by U.S. government organizations to protect sensitive (unclassified) information. Use this option to encrypt these links: – Server-to-gateway (H.248) – Gateway-to-endpoint (H.323) ● **aea** — Avaya Encryption Algorithm. Use this option as an alternative to AES 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. ● **SRTP** — All of the following 8 SRTP encryption options ***include authentication of RTCP*** with a 10- or 4-byte (80- or 32-bit) tag size. Encrypted RTCP is not currently supported. – **1-srtp-aescm128-hmac80** — AES encryption of RTP. Authentication of RTP with a 10-byte (80-bit) tag size. – **2-srtp-aescm128-hmac32** — AES encryption of RTP. Authentication of RTP with a 4-byte (32-bit) tag size. – **3-srtp-aescm128-hmac80-unauth** — AES encryption of RTP. No authentication of RTP. – **4-srtp-aescm128-hmac32-unauth** — AES encryption of RTP. No authentication of RTP. – **5-srtp-aescm128-hmac80-unenc** — No encryption of RTP. Authentication of RTP with a 10-byte (80-bit) tag size. – **6-srtp-aescm128-hmac32-unenc** — No encryption of RTP. Authentication of RTP with a 4-byte (32-bit) tag size. – **7-srtp-aescm128-hmac80-unenc-unauth** — No encryption or authentication of RTP. – **8-srtp-aescm128-hmac32-unenc-unauth** — No encryption or authentication of RTP. ● **none** — Media stream is unencrypted. This is the default setting.

2 of 2

3. Press **Next Page** to display page 2 of the screen.

   Page 2 appears.

IP-Codec-Set, page 2



```
change ip-codec-set n                                           Page   2 of   x

                             IP Codec Set

                                 Allow Direct-IP Multimedia? y
                 Maximum Call Rate for Direct-IP Multimedia: 384:Kbits
        Maximum Call Rate for Priority Direct-IP Multimedia: 384:Kbits


                    Mode        Redundancy

       FAX          relay          0
       Modem        off            0
       TDD/TTY      us             0
  Clear-channel     n              0
```

4. Complete the fields as described in the following table.

Table 13: IP Codec Set screen fields, page 2

Field	Conditions/Comments
All Direct-IP Multimedia?	Enter **y** to allow direct multimedia via the following codecs: ● H.261 ● H.263 ● H.264 (video) ● H.224 H.224.1 (data, far-end camera control).
Maximum Bandwidth Per Call for Direct-IP Multimedia	This field displays only when **Allow Direct-IP Multimedia** is **y**. Enter the unit of measure, **kbits** or **mbits**, corresponding to the numerical value entered for the bandwidth limitation. Default is **kbits**

1 of 4

Table 13: IP Codec Set screen fields, page 2 (continued)

Field	Conditions/Comments
FAX Mode	Specifies the mode for fax calls. Valid values are: ● **off** Turn off special fax handling when using this codec set. In this case, the fax is treated like an ordinary voice call. This setting could cause transmission errors or dropped calls. The pass-through setting is recommended if the codec set uses codecs other than G.711. For a codec set that uses G.711, this setting is required to send faxes to non-Avaya systems that do not support T.38 fax. ● **relay** For users in regions using this codec set, use Avaya relay mode for fax transmissions over IP network facilities. This is the default for new installations and upgrades to Communication Manager R2.1. ● **pass-through** For users in regions using this codec set, use pass-through mode for fax transmissions over IP network facilities. This mode uses G.711-like encoding. ● **t.38-standard** For users in regions using this codec set, use T.38 standard signaling for fax transmissions over IP network facilities.
	2 of 4

Table 13: IP Codec Set screen fields, page 2 (continued)

Field	Conditions/Comments
Modem Mode	Specifies the mode for modem calls. Valid values are: ● **off** Turn off special modem handling when using this codec set. In this case, the modem transmission is treated like an ordinary voice call. This is the default for new installations and upgrades to Communication Manager R2.1. This setting could cause transmission errors or dropped calls. The pass-through setting is recommended if the codec set uses codecs other than G.711. For a codec set that uses G.711, this setting is required to send modem calls to non-Avaya systems. ● **relay** For users in regions using this codec set, use relay mode for modem transmissions over IP network facilities. ● **pass-through** For users in regions using this codec set, use pass-through mode for modem transmissions over IP network facilities.
TDD/TTY Mode	Specifies the mode for TDD/TTY calls. Valid values are: ● **off** Turn off special TTY handling when using this codec set. In this case, the TTY transmission is treated like an ordinary voice call. This setting could cause transmission errors or dropped calls. The pass-through setting is recommended if the codec set uses codecs other than G.711. For a codec set that uses G.711, this setting is required to send TTY calls to non-Avaya systems. ● **US** For users in regions using this codec set, use U.S. Baudot 45.45 mode for TTY transmissions over IP network facilities. This is the default for new installations and upgrades to Communication Manager R2.1. ● **UK** For users in regions using this codec set, use U.K. Baudot 50 mode for TTY transmissions over IP network facilities. ● **pass-through** For users in regions using this codec set, use pass-through mode for TTY transmissions over IP network facilities.
	3 of 4

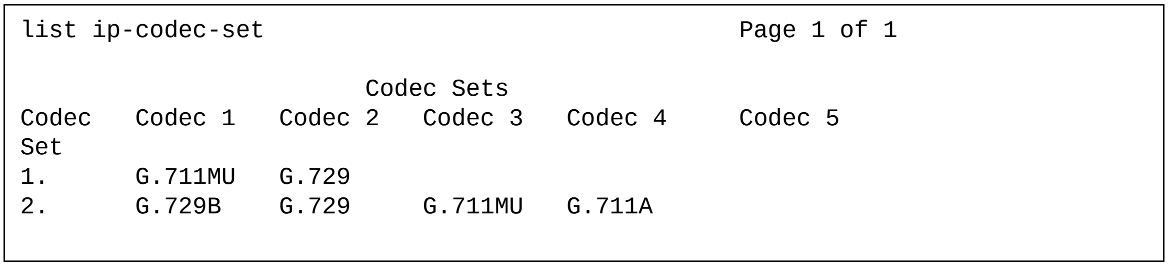
Table 13: IP Codec Set screen fields, page 2 (continued)

Field	Conditions/Comments
Clear Channel	● **"y"**es allows 64 kbps clear channel data calls for this codec set. ● **"n"**o disallows 64 kbps clear channel data calls for this codec set.
Redundancy	For the 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. **0** means that you do not want to send duplicated packets. For the clear-channel call type and call types for which you selected the pass-through mode, you can enter either 0 (do not use redundant payloads) or 1 (use redundant payloads).

4 of 4

5. Submit the screen.
6. Type **`list ip-codec-set`** and press **Enter** to list all CODEC sets on the **CODEC Set** screen.

Codec Sets screen



```
list ip-codec-set                                 Page 1 of 1

                        Codec Sets
Codec   Codec 1   Codec 2   Codec 3   Codec 4     Codec 5
Set
1.      G.711MU   G.729
2.      G.729B    G.729     G.711MU   G.711A
```

7. Review your CODEC sets.

Administering IP network regions

Network regions enable you to group IP endpoints and/or 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 Media Gateways. Some of the characteristics that can be defined for these IP endpoints and resources are:

- Audio Parameters
  - Codec Set
  - UDP port Range
  - Enabling Direct IP-IP connections
  - Enabling Hairpinning

- 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 on ip-network-region, see *Administering Avaya Aura™ Communication Manager 03-300509*.

The following sections tell you about:

- Defining an IP network region
- Setting up Inter-Gateway Alternate Routing (IGAR)
- Setting up Dial Plan Transparency
- Network Region Wizard (NRW)
- Manually interconnecting the network regions
- Administering inter-network region connections
- Pair-wise administration of IGAR between network regions
- Reviewing the network region administration

Note:

For more information on using network regions, with examples, see the application note *Network Regions for Avaya MultiVantage™ Solutions - A Tutorial*, which is available at: http://www.avaya.com/gcm/master-usa/en-us/resource/assets/applicationnotes/advantages_of_implem.pdf (requires Adobe Reader). For more information on configuring network regions in Communication Manager, see the application note *Avaya Aura™ Communication Manager Network Region Configuration Guide*, which is available at: http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/netw-region-tutorial.pdf (requires Adobe Reader).

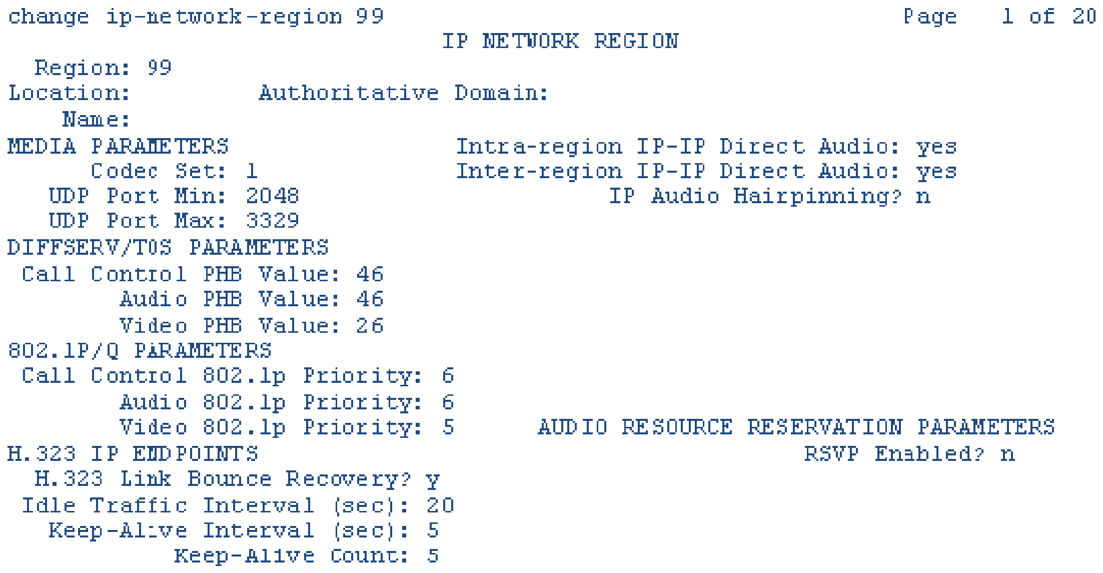
Defining an IP network region

CAUTION:
Never define a network region to span a WAN link.

To define an IP network region

1. Type **`change ip-network-region`** to open the **IP Network Region** screen.

Figure 15: IP Network Region screen



```
change ip-network-region 99                                     Page   1 of 20
                               IP NETWORK REGION
  Region: 99
Location:         Authoritative Domain:
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

2. Complete the fields using the information in Table 14: IP Network Region field descriptions on page 150.

Table 14: IP Network Region field descriptions

Field	Descriptions/Comments
Region	Network Region number, **1–250**.
Location	Blank or **1–250**. Enter the number for the location for the IP network region. The IP endpoint uses this as its location number. This applies to IP telephones and IP Softphones. **1-50** **1-250** **blank** The location is obtained from the cabinet containing the C-LAN that the endpoint registered through, or the media gateway containing the Internal Call Controller or Local Survivable Processor on an Avaya S8300D Server through which the endpoint registered. This applies to IP telephones and IP Softphones. Traditional cabinets, Remote Offices, and the Avaya S8300D Server all have their locations administered on their corresponding screens.
Name	Describes the region. Enter a character string up to 20 characters.
Home Domain	The network domain of the server.
AUDIO PARAMETERS	
Codec Set	Specifies the CODEC set assigned to a region. Enter a value between **1-7** (default is **1**). **Note:** CODEC sets are administered on the **CODEC Set** screen (see Administering IP CODEC sets).
UDP Port-Min	Specifies the lowest port number to be used for audio packets. Enter a value between **2-65406** (default is **2048**). **Note:** This number must be twice the number of calls that you want to support plus one, must start with an even number, and must be consecutive. Minimum range is 128 ports. ⚠ **CAUTION:** Avoid the range of “well-known” or IETF-assigned ports. Do not use ports below 1024.
	1 of 5

Table 14: IP Network Region field descriptions (continued)

Field	Descriptions/Comments
UDP Port-Max	Specifies the highest port number to be used for audio packets. Enter a value between **130-65535** (default is **65535**). ⚠ **CAUTION:** Avoid 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 have 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 appears 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 appears 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 appears only if the **802.1p/Q Enabled** field is **y**. The valid range is **0–7**.
H.323 IP ENDPOINTS	
H.323 Link Bounce Recovery	**y/n** Specifies whether to enable H.323 Link Bounce Recovery feature for this network region.
	2 of 5

Table 14: IP Network Region field descriptions (continued)

Field	Descriptions/Comments
Idle Traffic Interval (sec)	**5-7200** Enter the maximum traffic idle time in seconds. Default is **20**.
Keep-Alive Interval (sec)	**1-120** Specify the interval between KA retransmissions in seconds. Default is **5**.
Keep-Alive Count	**1-20** Specify the number of retries if no ACK is received. Default is **5**.
Intra-region IP-IP Direct Audio	**y/n** 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 direct IP-to-IP connections within the region is that of the IP telephone/IP Softphone itself (without being translated by NAT). IP phones 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 direct IP-to-IP connections within the region is to be the one with which a NAT device replaces the native address. IP phones must be configured behind a NAT device *before* this entry is enabled.
Inter-region IP-IP Direct Audio	**y/n** 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 phones 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 phones must be configured behind a NAT device *before* this entry is enabled.
IP Audio Hairpinning?	**y/n** Enter **y** to allow IP endpoints to be connected through the server's IP circuit pack in IP format, without first going through the Avaya TDM bus.
RTCP Reporting Enabled?	Specifies whether you want to enable RTCP reporting. If this field is set to **y**, then the RTCP Monitor Server Parameters fields appear.
	3 of 5

Table 14: IP Network Region field descriptions (continued)

Field	Descriptions/Comments
RTCP MONITOR SERVER PARAMETERs	
Use Default Server Parameters?	This field only appears when the **RTCP Reporting Enabled** field is set to **y**. ● Enter **y** to use the default RTCP Monitor server parameters as defined on the IP Options System Parameters screen. If set to **y**, you must complete the **Default Server IP Address** field on the **IP Options System Parameters** screen (`change system-parameters ip-options`). ● If you enter **n**, you need to complete the **Server IP Address**, **Server Port**, and **RTCP Report Period** fields.
Server IP Address	This field only appears when the **Use Default Server Address** field is set to **n** and the **RTCP Enabled** field is set to **y**. Enter the IP address for the RTCP Monitor server in **nnn.nnn.nnn.nnn** format, where **nnn=0-255.**
Server Port	This field only appears when the **Use Default Server Address** field is set to **n** and the **RTCP Enabled** field is set to **y**. Enter the port (**1-65535**) for the RTCP Monitor server.
RTCP Report Period (secs)	This field only appears when the **Use Default Server Address** field is set to **n** and the and the **RTCP Enabled** field is set to **y**. Range of values is **5-30** (seconds).
AUDIO RESOURCE RESERVATION PARAMETERS	
RSVP Enabled?	**y/n** Specifies whether or not you want to enable RSVP.
RSVP Refresh Rate (sec)	Enter the RSVP refresh rate in seconds (**1-99**). This field only appears if the **RSVP Enabled** field is set to **y.**
Retry upon RSVP Failure Enabled	Specifies whether to enable retries when RSVP fails (**y/n**). This field only appears if the **RSVP Enabled** field is set to **y.**
	4 of 5

Table 14: IP Network Region field descriptions (continued)

Field	Descriptions/Comments
RSVP Profile	This field only appears if the **RSVP Enabled** field is set to **y.** You set this field to what you have configured on your network ● **guaranteed-service** places a limit on the end-to-end queuing delay from the sender tot he receiver. This 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 in 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 appears if the **RSVP Enabled** field is set to **y.** **Note:** The "per-flow state and signaling" is RSVP, and 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.

5 of 5

⚠ **CAUTION:**

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

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

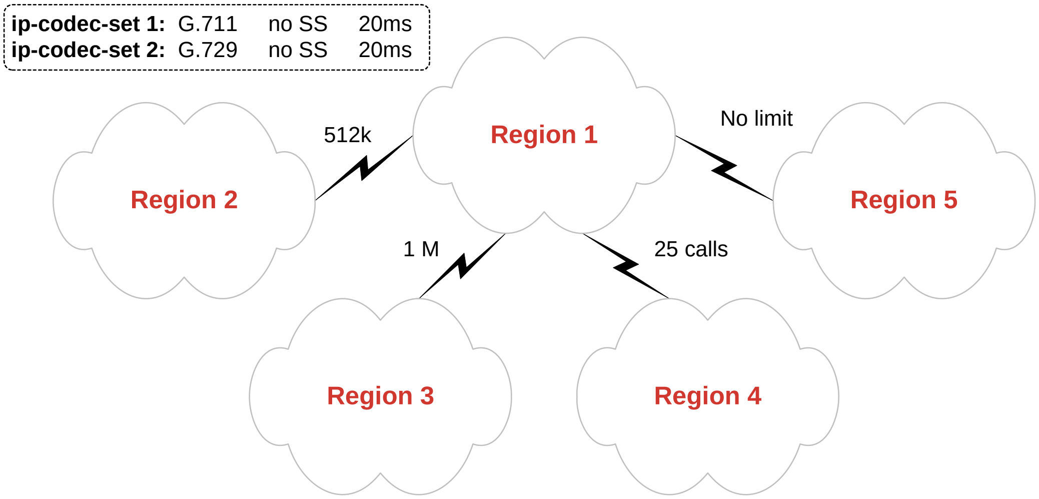
Call Admission Control

Call Admission Control (CAC) is a feature that allows a limit to be set 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. This is done by setting either a bandwidth limit or a number-of-calls limit between network regions, as follows:

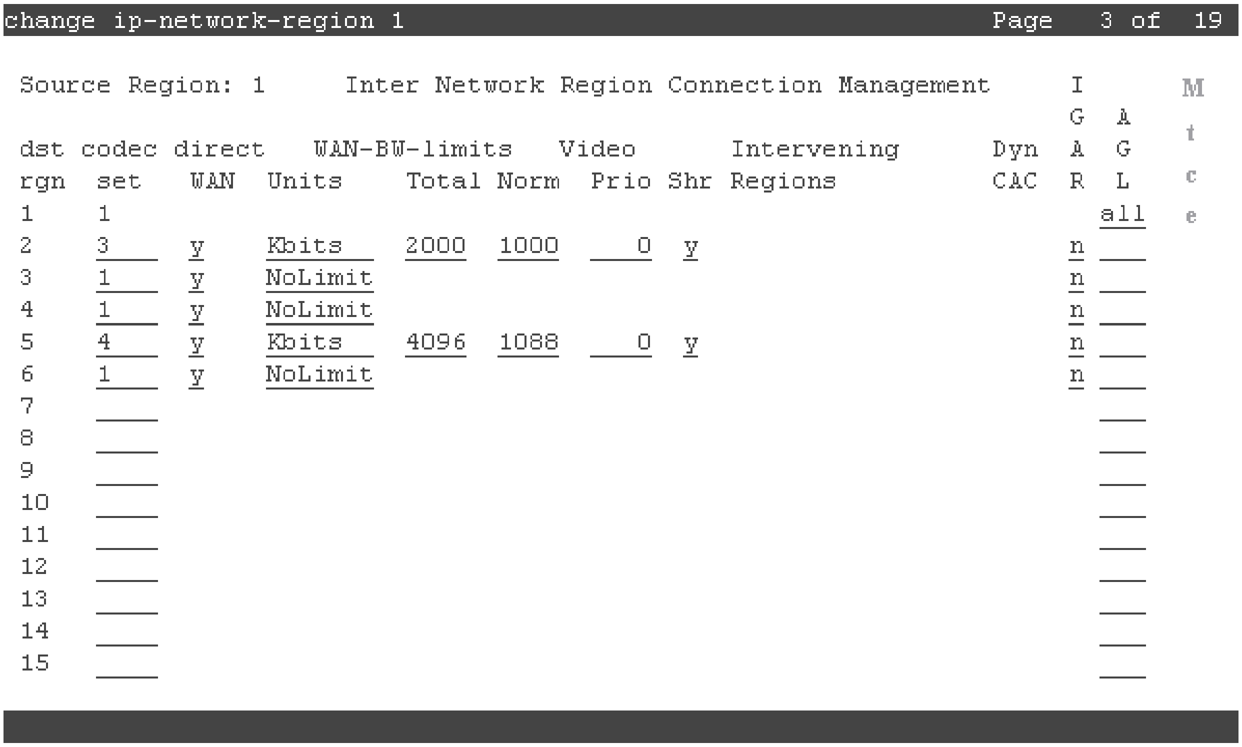
- Bandwidth consumption is calculated using the methodology explained in the *Avaya Application Solutions: IP Telephony Deployment Guide* (555-245-600).
- The L2 overhead is assumed to be 7 bytes, which is the most common L2 overhead size for WAN protocols.
- The calculated bandwidth consumption is rounded up to the nearest whole number.
- The calculated bandwidth consumption takes into account the actual IP CODEC being used for each individual call. It does not assume that all calls use the same CODEC.
- If the administrator chooses not to have the server calculate the bandwidth consumption, he/she may enter in 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 either all calls use the same CODEC, or that the manual limit takes into account the highest possible bandwidth consumption for the specified inter-region CODEC set.
- If a call between two network regions traverses an intervening network region (for example, a call from 1 to 3 actually goes 1 to 2 to 3), then the call server keeps track of the bandwidth consumed across both inter-region connections, that is, both 1 to 2 and 2 to 3.


ip-codec-set 1: G.711 no SS 20ms
ip-codec-set 2: G.729 no SS 20ms
Region 1
Region 2
Region 3
Region 4
Region 5
512k
No limit
1 M
25 calls

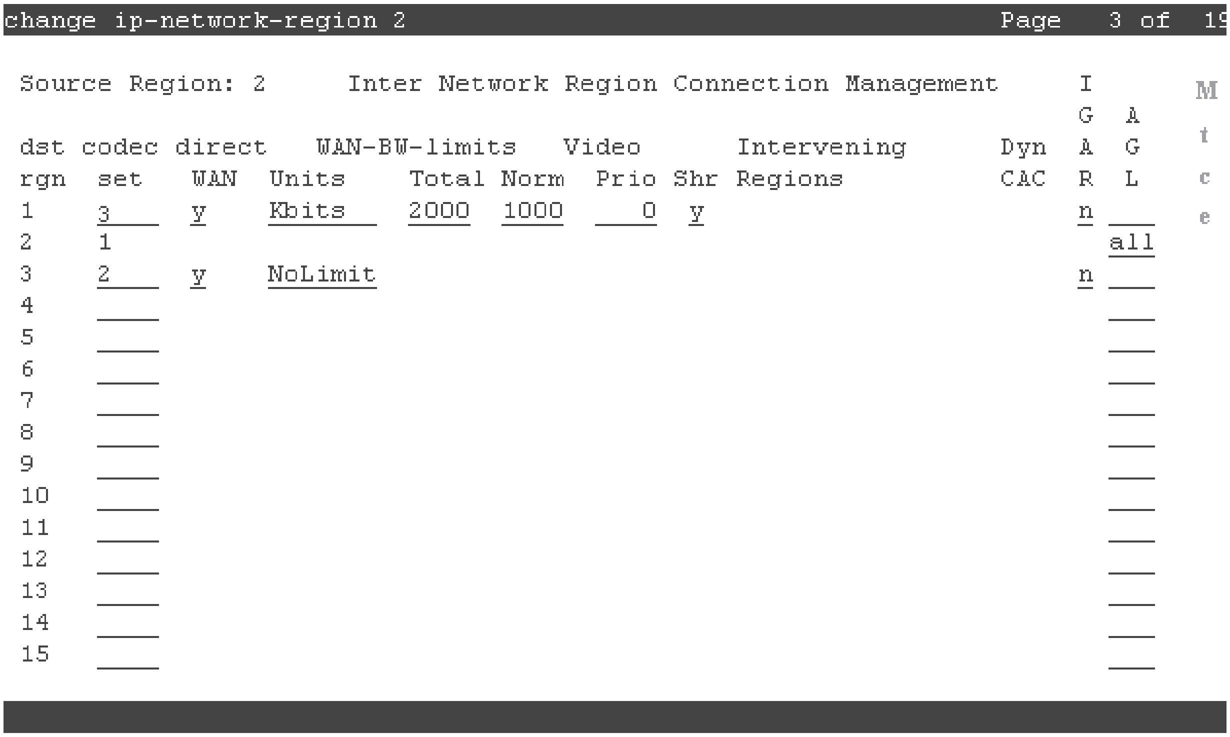
The figure above shows a simple hub-spoke network region topology. The WAN link between network regions 1 and 2 has 512kbps reserved for VoIP. The WAN link between network regions 1 and 3 has 1Mbps reserved for VoIP. The link between network regions 1 and 4 is one where the 7-byte L2 overhead assumption would not 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 20ms).

Therefore, it is feasible to set a limit on the number of inter-region calls to region 4, knowing 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.

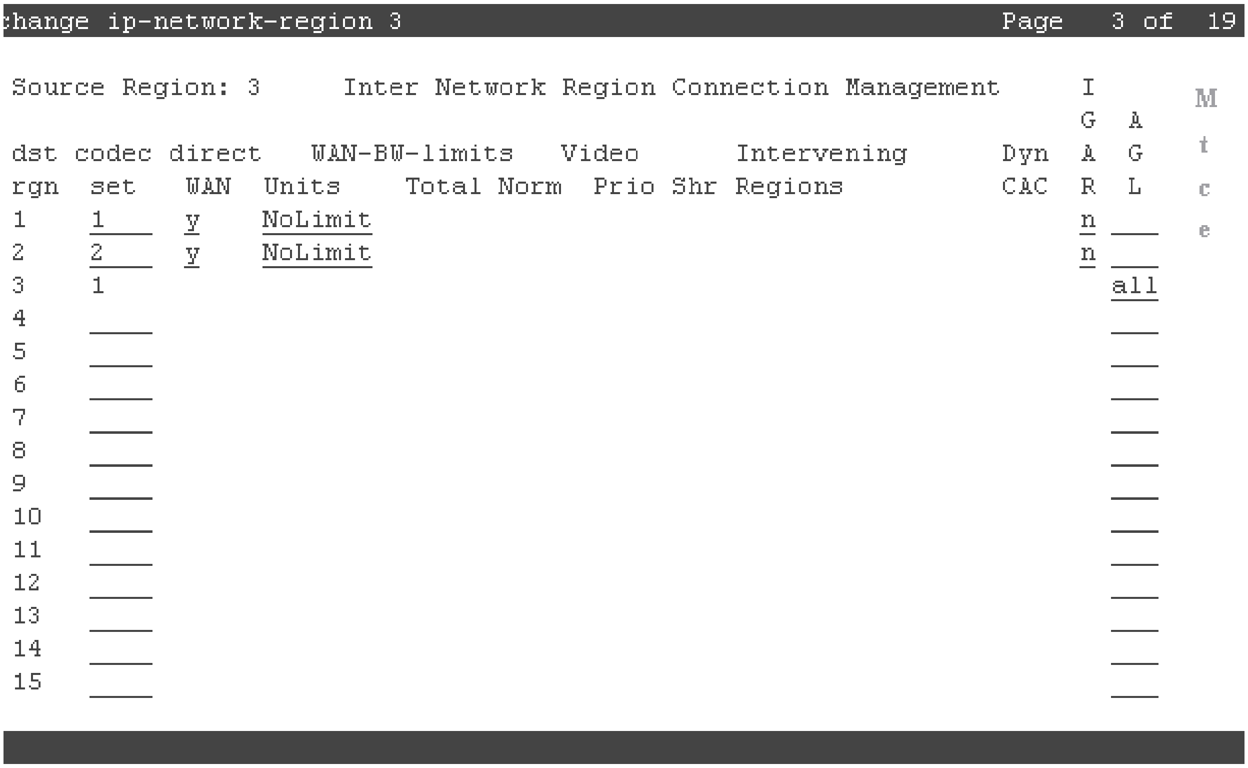
The corresponding **IP Network Region** screens for each network region are shown below.



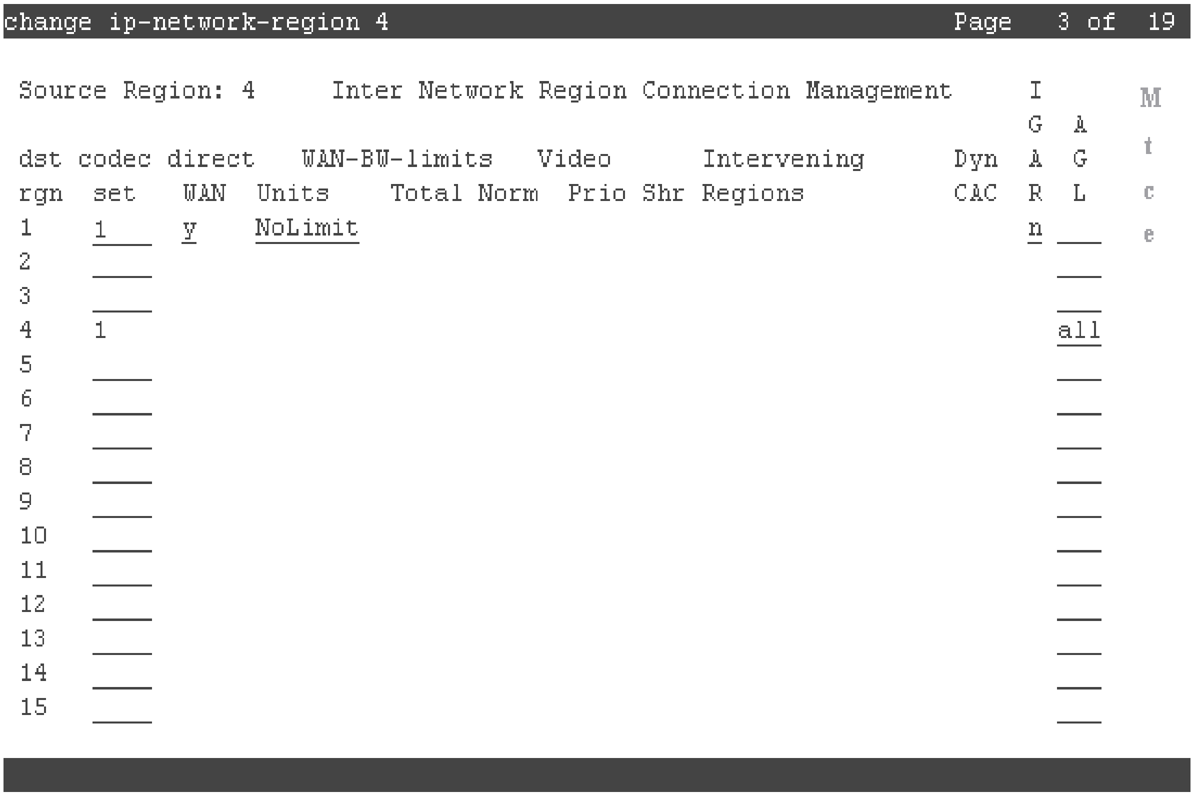
```
change ip-network-region 1                                        Page   3 of  19

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    t
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    c
 1    1                                                                 all  e
 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
```



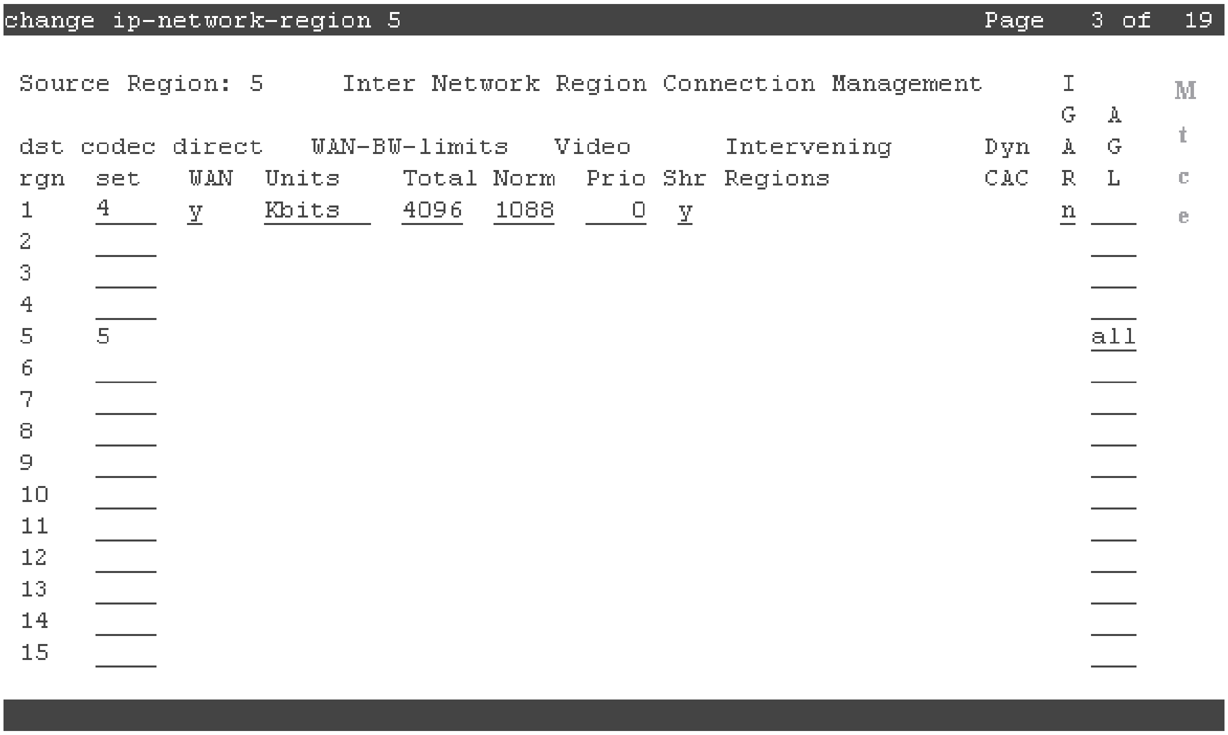
```
change ip-network-region 2                                      Page   3 of  19

 Source Region: 2     Inter Network Region Connection Management      I       M
                                                                      G  A
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn   A  G    t
 rgn  set   WAN  Units     Total Norm   Prio Shr Regions         CAC   R  L    c
 1    3____ y    Kbits___  2000  1000   ___0  y                        n ___   e
 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
dst codec direct   WAN-BW-limits   Video      Intervening      Dyn   A  G    t
rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC   R  L    c
1    1     y    NoLimit                                              n       e
2    2     y    NoLimit                                              n
3    1                                                                  all
4
5
6
7
8
9
10
11
12
13
14
15
```



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

 Source Region: 4     Inter Network Region Connection Management     I       M
                                                                     G  A
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    t
 rgn  set    WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    c
 1    1___  y    NoLimit                                             n ___   e
 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
 dst  codec direct   WAN-BW-limits   Video       Intervening      Dyn  A  G      t
 rgn   set    WAN  Units     Total Norm  Prio Shr Regions         CAC  R  L      c
 1     4____  y    Kbits___  4096  1088  ___0  y                       n  ___    e
 2     _____                                                              ___
 3     _____                                                              ___
 4     _____                                                              ___
 5     5                                                                  all
 6     _____                                                              ___
 7     _____                                                              ___
 8     _____                                                              ___
 9     _____                                                              ___
 10    _____                                                              ___
 11    _____                                                              ___
 12    _____                                                              ___
 13    _____                                                              ___
 14    _____                                                              ___
 15    _____                                                              ___
```

Effect of Video on Call Admission Control and Bandwidth Management

Multimedia calls are initiated with voice and video. Once a call is established, one of the parties can initiate an associated data conference to include all the parties on the call who are capable of supporting data.

For more information on managing video on your network, see *Avaya Video Conferencing Solutions Networking Guide*.

With Communication Manager Release 6.0, you can use cumulative bandwidth management to set video bandwith for the Avaya Video Telephony Solution. The Audio Call Admission Control capability allows you to set maximum bandwidth between multiple network regions for audio calls. Video bandwidth can also be controlled in a similar way.

Avaya recommends the following for calls with voice and video:

- Put video and audio endpoints into separate network regions. Consider these separate network regions as physical locations.
- Assign higher average bandwidth per call appropriate to video endpoints.

- If video endpoint bandwidths differ greatly, create several video network regions, for example, video phones versus room systems.

Note:
Calls from a video network region is assigned video bandwidth, even if users place audio only calls. This results in some bandwidth wastage.
Calls between audio and video network regions(either direction) are assigned two bandwidths - audio average bandwidth charged to audio network and video average bandwidth charged to video network.

For Communication Manager 6.0, the total bandwidth can be partitioned as:

- Conservative (assuming audio is mission-critical): Assign enough bandwidth for maximum concurrent audio calls to video network regions. Assign the remaining bandwidth to video.
- Aggressive - From the actual available bandwidth, find the total of the bandwidth assigned to audio or video network regions. If an audio or video burst call occurs, users will experience inferior quality.

Note:
The audio and video network regions cannot borrow bandwidth from each other.

Setting up Inter-Gateway Alternate Routing (IGAR)

Whenever the Communication Manager software needs an inter-gateway connection and sufficient IP bandwidth is not available, it attempts to substitute a trunk connection for the IP connection. This happens in any of a large variety of scenarios, including the following examples:

- A party in one Network Region (NR) calls a party in another NR, or
- A station in one NR bridges onto a call appearance of a station in another NR, or
- An incoming trunk in one NR routes to a hunt group with agents in another NR, or
- An announcement or music source from one NR must be played to a party in another NR.

Communication Manager software automatically attempts to use a trunk for inter-region voice bearer connection when *all* of the following five conditions are met:

- An inter-gateway connection is needed.
- IGAR has been “triggered” by one (or more) of the following conditions:
  - The administered bandwidth limit between two NRs has been exhausted, or
  - The VoIP resources between two PN/MGs have been exhausted, or
  - IGAR has been “forced” between two NRs, or
  - The codec set is set to pstn.
- IGAR is enabled for the NRs associated with each end of the call.
- The System Parameter **Enable Inter-Gateway Alternate Routing** is set to ‘y’. See Figure 18.
- The number of trunks used by IGAR in each of the two NRs has not reached the limit administered for that NR.

A Trunk IGC is established using ARS to route a trunk call from one NR to the *IGAR LDN Extension* administered for other NR. Because the Trunk IGC is independent of the actual call being placed, Communication Manager can originate the IGC in either direction — that is, from the calling party’s NR to the NR of the called party, or vice versa. However, because some customers wish to use Facility Restriction Levels or Toll Restriction to determine who gets access to IGAR resources during a WAN outage, the calling user is considered the originator of the Trunk IGC for the purposes of authorization (for example, FRL checking) and routing (for example, determining which Location-specific ARS and Toll tables to use). However, if the outgoing trunk group is administered to send the Calling Number, the *IGAR Extension* in the originating NR is used to create this number using the appropriate administration (performed on the public/unknown or private numbering screen).

The following are examples of certain failure conditions and how Communication Manager handles them:

- On a direct call, the call proceeds to the first coverage point of the unreachable called endpoint, or if no coverage path is assigned, busy tone is played to the calling party.
- If the unreachable endpoint is being accessed through a coverage path, it is skipped.
- If the unreachable endpoint is the next available agent in a hunt group, that agent is considered unavailable, and the system tries to terminate to another agent using the administered group type (Circular, Percent Allocation Distribution, etc.).

Setting up Dial Plan Transparency

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

DPT does not need to be activated in the license file. DPT is available as a standard feature for Communication Manager Release 4.0 and later.

DPT is similar to IGAR in that they both provide alternate routing of calls when normal connections are not available. A major difference between DPT and IGAR is that DPT routes calls between endpoints controlled by two independent servers while IGAR routes calls between endpoints controlled by a single server. The DPT and IGAR features are independent of each other but can be activated at the same time.

Limitations of DPT include the following:

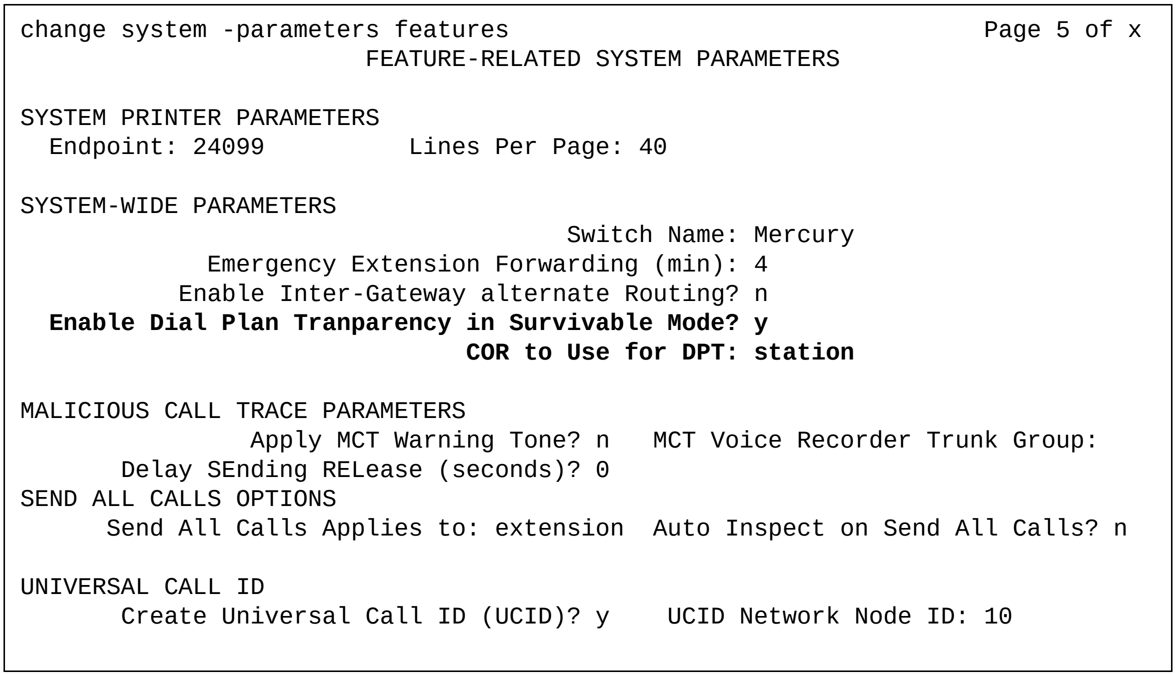
- DPT only handles IP network connectivity failures *between* network regions.
- Because DPT calls are trunk calls, many station features are not supported.
- For Release 4.0, DPT applies only to endpoints that are dialed directly. Redirected calls or calls to groups cannot be routed by DPT.
- DPT cannot reroute calls involving a SIP endpoint that has lost registration with its Home SM.
- Failover strategies for gateways and port networks, and alternate gatekeeper lists for IP stations, must be kept consistent for DPT to work.

Use the following procedure to administer DPT

1. Enable DPT on the Feature-Related System Parameters screen
   a. set **Enable Dial Plan Transparency in Survivable Mode** to **y**.
   b. Set **COR to Use for DPT** to either **station** or **unrestricted**.

      If set to **station**, the Facility Restriction Level (FRL) of the calling station determines whether that station is permitted to make a trunk call and if so, which trunks it is eligible to access. If set to **unrestricted**, the first available trunk preference pointed to by ARS routing is used.

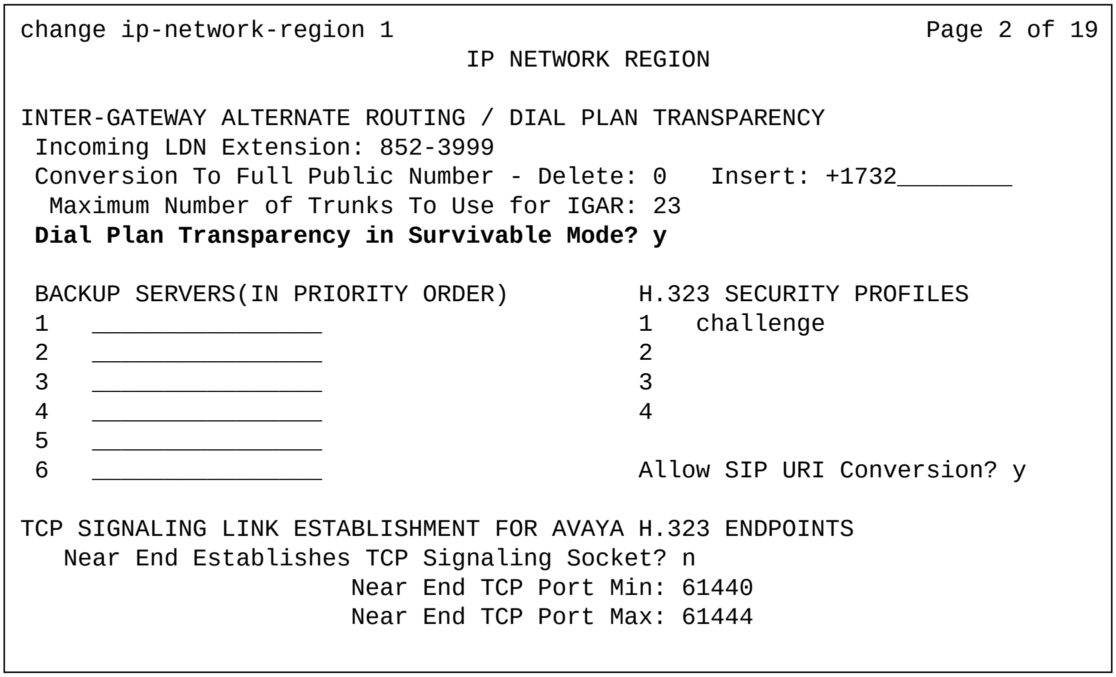
Figure 16: Enabling DPT on the System Features screen



```
change system -parameters features                                 Page 5 of x
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint: 24099          Lines Per Page: 40

SYSTEM-WIDE PARAMETERS
                                      Switch Name: Mercury
             Emergency Extension Forwarding (min): 4
           Enable Inter-Gateway alternate Routing? n
  Enable Dial Plan Tranparency in Survivable Mode? y
                               COR to Use for DPT: station

MALICIOUS CALL TRACE PARAMETERS
                Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
       Delay SEnding RELease (seconds)? 0
SEND ALL CALLS OPTIONS
      Send All Calls Applies to: extension  Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
       Create Universal Call ID (UCID)? y    UCID Network Node ID: 10
```

2. Enable DPT for the appropriate Network Regions. On page 2 of the IP Network Region screen, set the **Dial Plan Transparency in Survivable Mode** field to **y**.

Figure 17: Enabling DPT on the Network Region screen



```
change ip-network-region 1                                     Page 2 of 19
                               IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY
 Incoming LDN Extension: 852-3999
 Conversion To Full Public Number - Delete: 0   Insert: +1732________
  Maximum Number of Trunks To Use for IGAR: 23
 Dial Plan Transparency in Survivable Mode? y

 BACKUP SERVERS(IN PRIORITY ORDER)         H.323 SECURITY PROFILES
 1   ________________                      1   challenge
 2   ________________                      2
 3   ________________                      3
 4   ________________                      4
 5   ________________
 6   ________________                      Allow SIP URI Conversion? y

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Socket? n
                       Near End TCP Port Min: 61440
                       Near End TCP Port Max: 61444
```

3. If not already completed for IGAR, allocate on incoming DID / LDN extension for incoming DPT calls. This extension can be shared by IGAR and DPT.
4. As for IGAR, ensure that a sufficient number of trunks are available. You do not need to set the maximum number of trunks for DPT.
5. Use existing routing techniques to ensure that an outgoing DPT call from a given Network Region has access to an outgoing trunk. The outgoing trunk need not be in the same Network Region as the calling endpoint, as long as the endpoint and trunk Network Regions are interconnected.

Network Region Wizard (NRW)

The Avaya Network Region Wizard (NRW) is a browser-based wizard that is available on Avaya Servers running Communication Manager 2.1 or higher software. The NWR supports IGAR along with prior support for CAC and codec set selection for inter-connected region pairs. For any system that has several network regions, the use of the wizard can save time for the software specialist or business partner provisioning the system, as well as help to configure the system for optimum IP performance.

The NRW guides you through the steps required to define network regions and set all necessary parameters through a simplified, task-oriented interface. The purpose of the NRW is to simplify and expedite the provisioning of multiple IP network regions, including Call Admission Control via Bandwidth Limits (CAC-BL) for large distributed single-server systems that have several network regions. The NRW is especially valuable for provisioning systems with dozens or hundreds of 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 (intra-region) LANs and lower-bandwidth (inter-region) WANs
- Configuration of IP network regions, including all intra-region settings, as well as inter-region administration of CAC-BL for inter-region links
- Ongoing network region administration by the customer as well as by Avaya technicians and Business Partners to accommodate changes in the customer network following cutover
- Assignment of VoIP resources (C-LANs, TN2302/TN2602 circuit packs, Media Gateways), and endpoints to IP network regions.

The NRW simplifies and expedites network region provisioning in several ways:

- NRW uses algorithms and heuristics based on graph theory to greatly reduce the repetitive manual entry required by the SAT to configure codecs, and CAC-BL for inter-region links. With the SAT, the number of inter-region links that need to be configured by the user does not scale well; with the NRW, the number of region pairs that require manual administration will increase *linearly* with the number of regions.

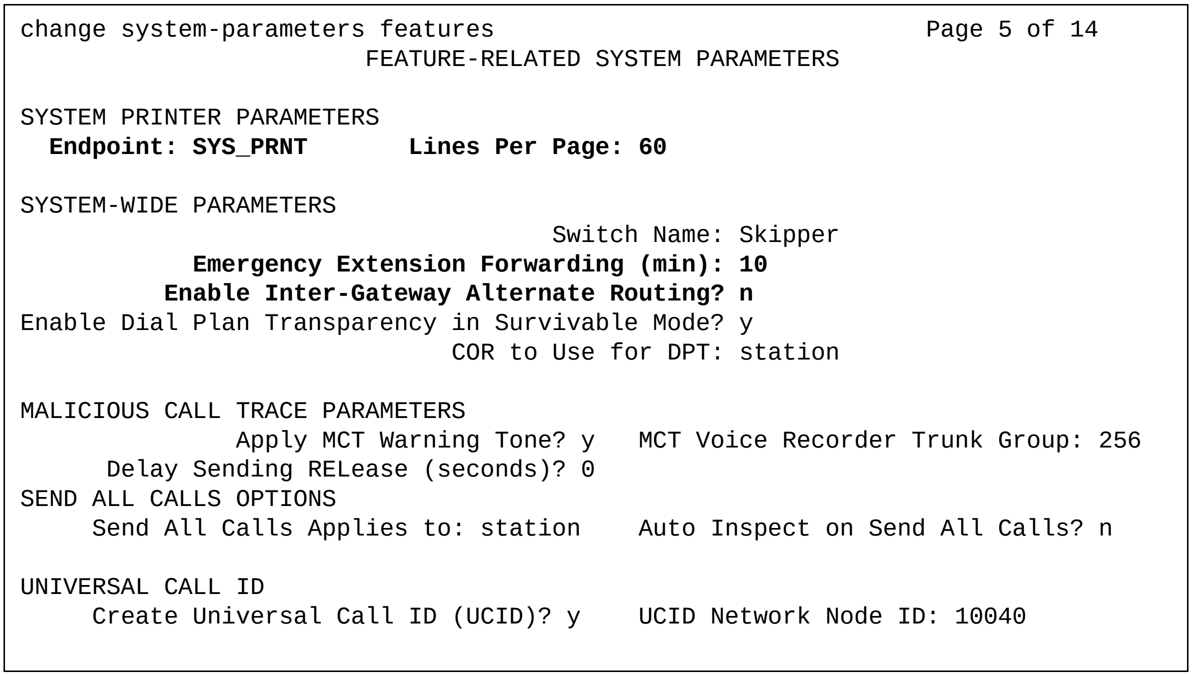
- NRW provides templates of widely applicable default values for codec sets and intra-region parameter settings. Users have the ability to customize these templates with their own default values.
- NRW runs on any Internet browser supported by the Avaya Integrated Management (IM) product line, and takes advantage of browser capabilities to offer user-friendly prompting and context-sensitive online help.

The NRW has its own Job Aid and worksheet (one of Avaya's wizard tools that are available from http://support.avaya.com/avayaiw), and is a standard IM support tool delivered with every Linux-based Communication Manager system.

Manually interconnecting the network regions

Use the **Enable Inter-Gateway Alternate Routing**? field on the Feature-Related System Parameters screen to enable IGAR on a system-wide basis. Using this parameter, IGAR can be quickly disabled without changing/removing other feature administration associated with IGAR. This parameter is included under the **System-Wide Parameters**, as shown in Figure 18.

Figure 18: IGAR system parameter



```
change system-parameters features                               Page 5 of 14
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint: SYS_PRNT       Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                     Switch Name: Skipper
            Emergency Extension Forwarding (min): 10
          Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? y
                              COR to Use for DPT: station

MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? y   MCT Voice Recorder Trunk Group: 256
      Delay Sending RELease (seconds)? 0
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? y    UCID Network Node ID: 10040
```

If TN799DP (C-LAN) and TN2302AP (IP Media Processor) resources are shared between/among administered network regions, you must define which regions communicate with which other regions and with what CODEC set on the **Inter-Network Region Connection Management** screen (**`change/display/status ip-network-region`**).

Note:
You cannot connect IP endpoints in different network regions or communicate between/among network regions unless you specify the CODEC set on this screen.

You can also specify for the *Call Admission Control - Bandwidth Limitation* feature:

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

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

  Typically, the bandwidth limit is specified as the number of calls when the codec set administered across a WAN link contains a single codec. 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 on using network regions, with examples, see the application note *Network Regions for Avaya MultiVantage™ Solutions - A Tutorial*, which is available at: http://www.avaya.com/gcm/master-usa/en-us/resource/assets/applicationnotes/advantages_of_implem.pdf (requires Adobe Reader). For more information on configuring network regions in Communication Manager, see the application note *Avaya Aura™ Communication Manager Network Region Configuration Guide*, which is available at: http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/netw-region-tutorial.pdf (requires Adobe Reader). For information on using the Network Region Wizard, see the *Network Region Job Aid*, 14-300283, which is available at http://www.avaya.com/support.

Administering inter-network region connections

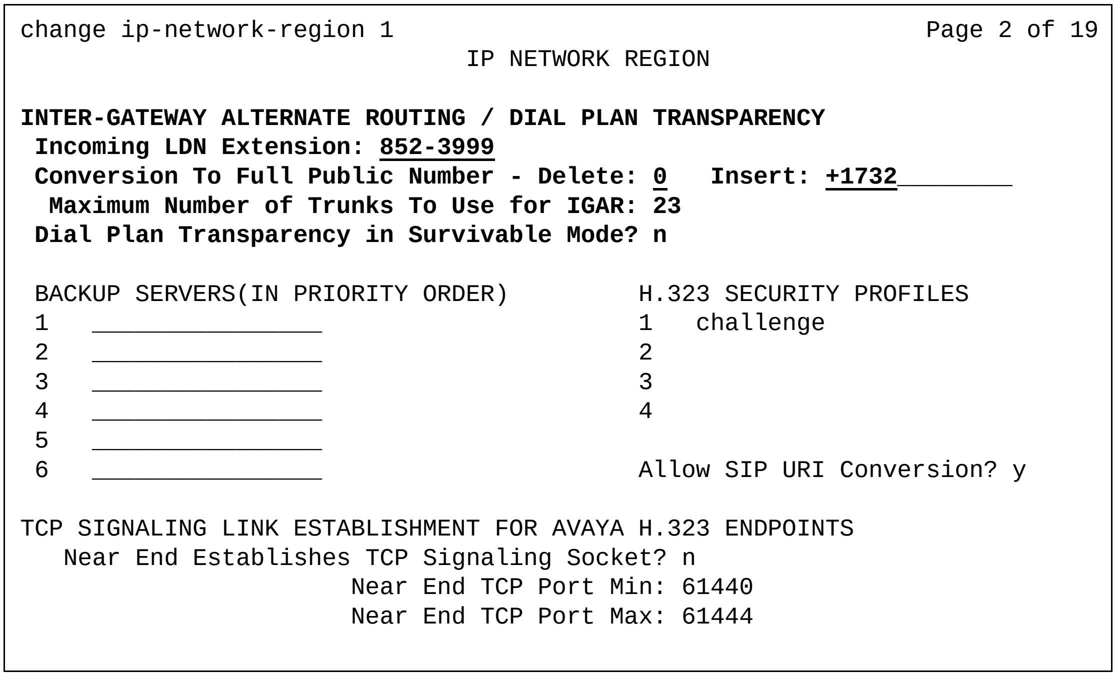
An **Alternate Routing Extension** field has been added to the second page of the **IP Network Region** screen. This unassigned extension (up to 7 digits long), together with two other fields are required for each network region in order to route the bearer portion of the IGAR call. The following must be performed:

- If IGAR is enabled for any row on pages 3 through 19, then the user shall be:
  - Required to enter an IGAR extension before submitting the screen
  - Blocked from blanking out a previously administered IGAR extension
- If IGAR is disabled by the System Parameter, the customer is warned if any of these fields are updated.

The warning is "WARNING: The IGAR System Parameter is disabled."

Type **`change ip-network-region`** *#* and press **Enter** to open the **Inter Network Region Connection Management** screen. Go to Page 2.

Figure 19: Alternate Routing Extension field



```
change ip-network-region 1                                     Page 2 of 19
                               IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY
 Incoming LDN Extension: 852-3999
 Conversion To Full Public Number - Delete: 0   Insert: +1732________
  Maximum Number of Trunks To Use for IGAR: 23
 Dial Plan Transparency in Survivable Mode? n

 BACKUP SERVERS(IN PRIORITY ORDER)        H.323 SECURITY PROFILES
 1   ________________                     1   challenge
 2   ________________                     2
 3   ________________                     3
 4   ________________                     4
 5   ________________
 6   ________________                     Allow SIP URI Conversion? y

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Socket? n
                       Near End TCP Port Min: 61440
                       Near End TCP Port Max: 61444
```

Pair-wise administration of IGAR between network regions

An **IGAR** column has been added to the **IP Network Region** screen to allow 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 it is set to “n” the IGAR capability is disabled between the network region pair.

The following screen validations must be performed:

- If no IGAR Extension is administered on page 2 of the **IP Network Region** screen, the user is blocked from submitting the screen, if any network region pair has IGAR enabled.
- If IGAR is disabled using the System Parameter, the customer will be warned, if IGAR is enabled for any network region pair.

  The warning is “WARNING: The IGAR System Parameter is disabled.”

Normally, the administration between Network Region pairs would have a codec set identified for compressing voice across the IP WAN. Only if bandwidth in the IP WAN is exceeded, and the **IGAR** field is set to “y”, would the voice bearer be routed across an alternate trunk facility. However, under some conditions you may wish to 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 may also be used to move traffic off of the IP WAN temporarily, if an edge router is having problems, or an edge router needs to be replaced between a Network Region pair.

When the codec set type is set to “pstn” the following fields are defaulted:

- **IGAR** field defaults to “y”. Options: f(orced), n(o), y(es).

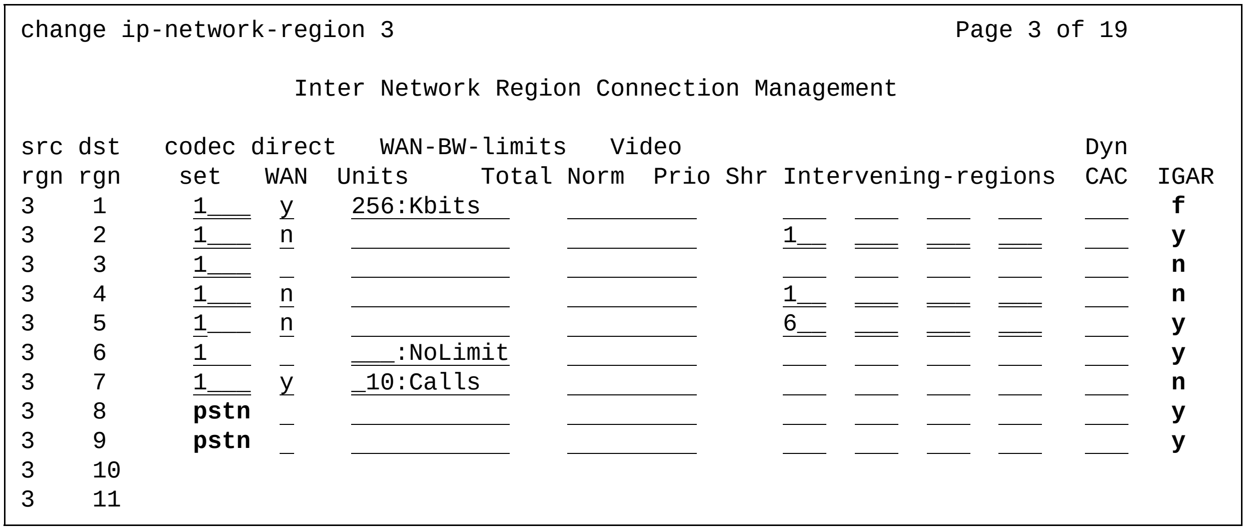
  This field must be defaulted to “y” because the Alternate Trunk Facility is the only means of routing the voice bearer portion of the call.

- When the codec set is set to “pstn” the following fields are hidden:
  - Direct-WAN
  - WAN-BW Limits, and
  - Intervening Regions

When the codec set is not “pstn” and not blank, the IGAR field is defaulted to “n”.

A “f(orced)” option is supported in the **IGAR** column in addition to the options “n(o)” and “y(es)”.

Figure 20: Inter network region connection management



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

                   Inter Network Region Connection Management

src dst   codec direct   WAN-BW-limits   Video                            Dyn
rgn rgn    set   WAN  Units     Total Norm  Prio Shr Intervening-regions  CAC  IGAR
3    1      1___  y    256:Kbits__    _________      ___  ___  ___  ___   ___   f
3    2      1___  n    ___________    _________      1__  ___  ___  ___   ___   y
3    3      1___  _    ___________    _________      ___  ___  ___  ___   ___   n
3    4      1___  n    ___________    _________      1__  ___  ___  ___   ___   n
3    5      1___  n    ___________    _________      6__  ___  ___  ___   ___   y
3    6      1___  _    ___:NoLimit    _________      ___  ___  ___  ___   ___   y
3    7      1___  y    _10:Calls__    _________      ___  ___  ___  ___   ___   n
3    8      pstn  _    ___________    _________      ___  ___  ___  ___   ___   y
3    9      pstn  _    ___________    _________      ___  ___  ___  ___   ___   y
3    10
3    11
```

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

In the example, network region 3 is directly connected to regions 6, and 7, and is indirectly connected to regions 2 and 4 (through region 1) and 5 (through region 6).

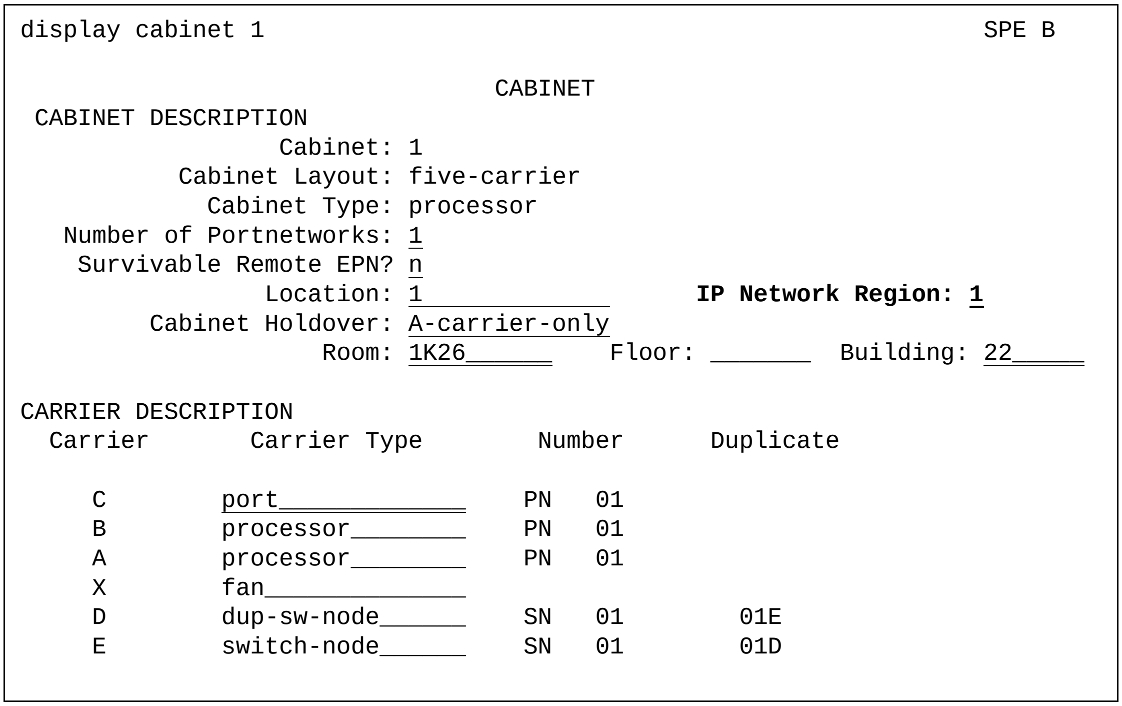
Press **Enter** to save the changes.

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. When an IP connection between two port network/media gateways (PN/MGs) cannot be established, the system tries to establish an IGAR trunk connection between the two PN/MGs. The system tries to use trunks in the specific PN/MG requested. However, because Communication Manager does not require every PN/MG to have PSTN trunks, it may be necessary to obtain trunks from another PN/MG. The system may only obtain trunks from a PN/MG in the same Network Region as the one in which the original request was made. This means Communication Manager must let customers associate a port network with a Network Region. This can already be done with Media Gateways.

Figure 21: IP network region field on cabinet screen to map PNs to network regions



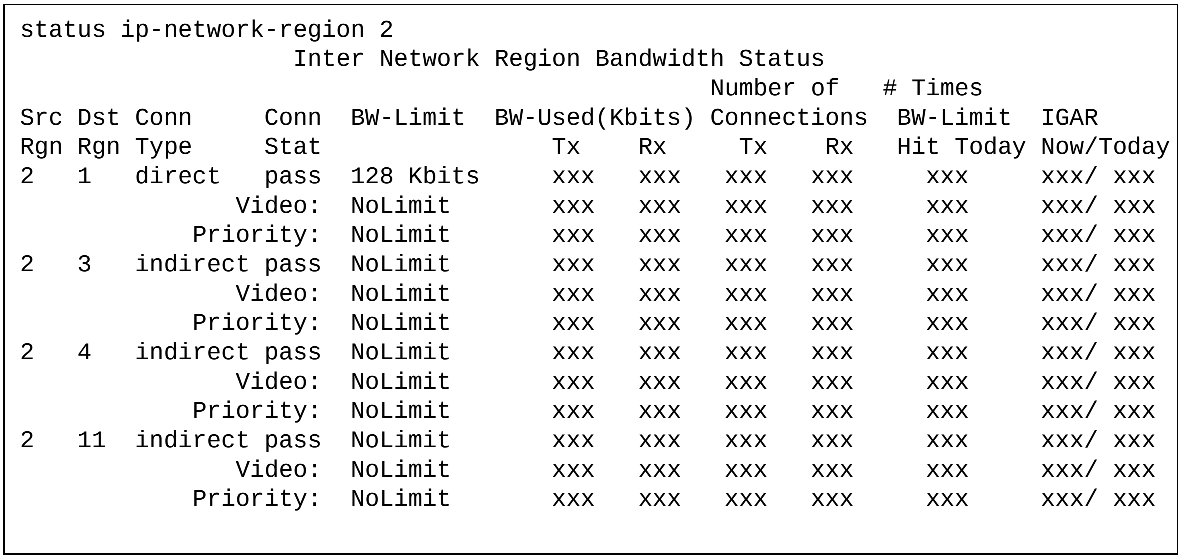
```
display cabinet 1                                                  SPE B

                                 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
```

Status of inter-region usage

You can check the status of bandwidth usage between network regions using: **`status ip-network-region`** ***`n`*** or ***`n/m`***. Using the ***`n`***, the connection status, bandwidth limits, and bandwidth usage is displayed for all regions directly connected to ***`n`***. For regions indirectly connected to ***`n`***, just the connection status is displayed. If regions ***`n`*** and ***`m`*** are indirectly connected, using ***`n/m`*** in 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 has been invoked for a network region pair, as shown in Figure 22. Type **`status ip-network-region`** ***`n`***, and press **Enter** to display the **Inter Network Region Bandwidth Status** screen.

Figure 22: IP network region status screen



```
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
```

The numbers in the column titled “IGAR Now/Today” have the following meanings:

- The first number (up to 3 digits or 999) displays the number of active IGAR connections for the pair of network regions at the time the command was invoked.
- The second number (up to 3 digits or 999) displays the number of times IGAR has been invoked for the pair of network regions since the previous midnight.

To administer the network region on the Signaling Group screen

Note:

> The S8300D Server in Survivable Remote server mode does not support signaling groups.

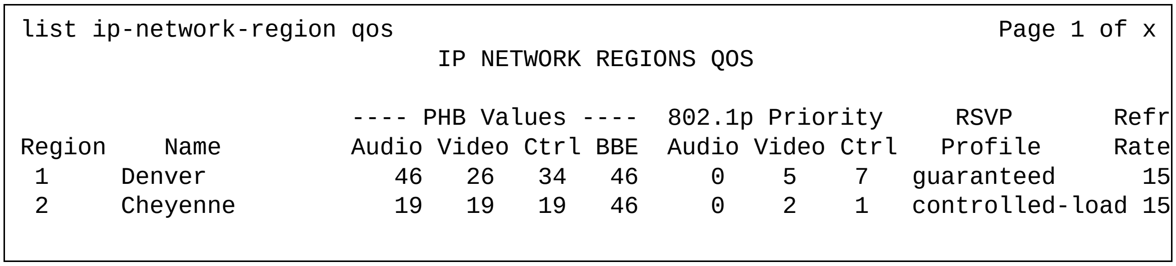
1. Type **change `signaling-group`** ***`group#`*** and press **Enter** to display the **Signaling Group** screen.

2. Type the number of the network region that corresponds to this signaling group in the **Far-end Network Region** field. The range of values is: **1-250**.
3. Press **Enter** to save the changes.

Reviewing the network region administration

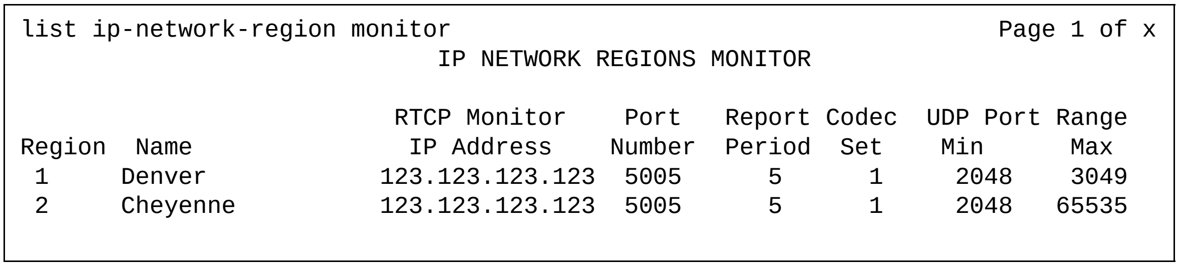
To check the network region administration:

1. Type **`list ip-network-region qos`** and press **Enter** to display the **IP Network Regions QOS** screen.



```
list ip-network-region qos                                         Page 1 of x
                             IP NETWORK REGIONS QOS

                       ---- PHB Values ----  802.1p Priority     RSVP       Refr
Region    Name         Audio Video Ctrl BBE  Audio Video Ctrl   Profile     Rate
 1     Denver             46    26   34   46     0     5    7   guaranteed      15
 2     Cheyenne           19    19   19   46     0     2    1   controlled-load 15
```

2. Ensure that you have the proper values for each network region and that the regions are interconnected according to your design.
3. Type **`list ip-network-region monitor`** and press **Enter** to see the **IP Network Regions Monitor** screen, which includes information about the CODEC sets.



```
list ip-network-region monitor                                     Page 1 of x
                             IP NETWORK REGIONS MONITOR

                          RTCP Monitor    Port   Report Codec  UDP Port Range
Region  Name               IP Address    Number  Period  Set    Min       Max
 1     Denver            123.123.123.123  5005      5      1     2048    3049
 2     Cheyenne          123.123.123.123  5005      5      1     2048   65535
```

4. Ensure that the audio transport parameters are administered according to your design.

Setting network performance thresholds

Note:
The *craft* (or higher) login is required to perform this administration.

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

Note:

You cannot administer these parameters unless these conditions are met:

- The **Group Type** field on the **Signaling Group** screen is **h.323** or **sip**.
- The **Bypass If IP Threshold Exceeded** field is set to **y** on the **Signaling Group** screen.

  If bypass is activated for a signaling group, ongoing measurements of network activity collected by the system are compared with the values in the **IP-options system-parameters** screen. If the values of these parameters are exceeded by the current measurements, the bypass function terminates further use of the network path associated with 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 are not allowed to arrive at the IP trunks on the bypassed signaling group and are diverted to alternate routes.
  - Outgoing calls are blocked on this signaling group.

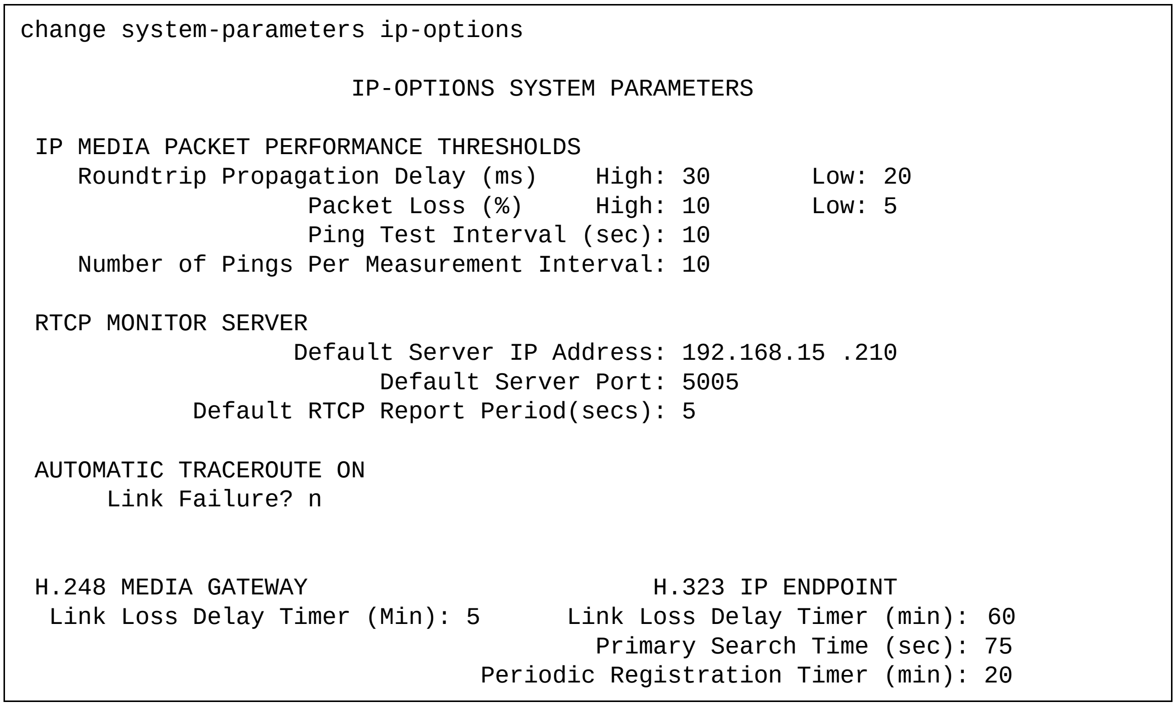
    If so administered, blocked calls are diverted to alternate routes (either IP or circuits) as determined by the administered routing patterns.

Note:

Avaya strongly recommends that you use the default values.

To administer network performance parameters

1. Enter **`change system-parameters ip-options`** to open the **IP Options System Parameters** screen.



```
change system-parameters ip-options

                       IP-OPTIONS SYSTEM PARAMETERS

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)    High: 30       Low: 20
                    Packet Loss (%)     High: 10       Low: 5
                    Ping Test Interval (sec): 10
    Number of Pings Per Measurement Interval: 10

 RTCP MONITOR SERVER
                   Default Server IP Address: 192.168.15 .210
                         Default Server Port: 5005
            Default RTCP Report Period(secs): 5

 AUTOMATIC TRACEROUTE ON
      Link Failure? n


 H.248 MEDIA GATEWAY                        H.323 IP ENDPOINT
  Link Loss Delay Timer (Min): 5      Link Loss Delay Timer (min):  60
                                        Primary Search Time (sec): 75
                                Periodic Registration Timer (min): 20
```

2. Enter values for the fields suitable for your network needs (defaults shown in the table below).

Field	Conditions/
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**

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

Enabling spanning tree protocol (STP)

Spanning Tree Protocol (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is to always leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) can lead to a complete cessation of all traffic.

However, STP is slow to converge after a network failure, and slow to allow a new port into the network (~50 sec by default).

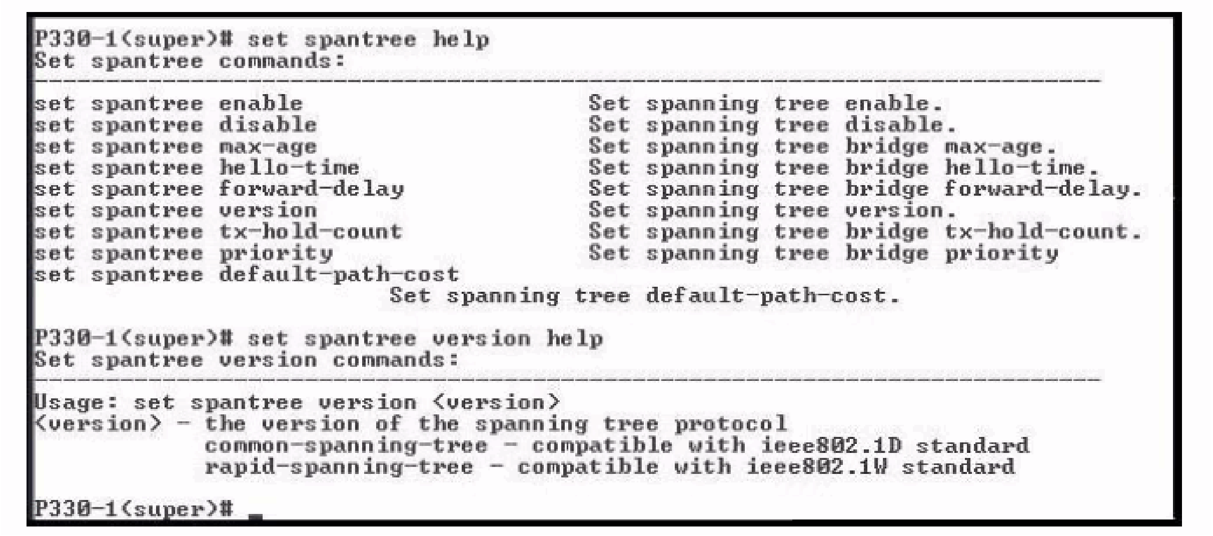
A modified version of STP, Rapid Spanning Tree converges faster than the earlier STP, and enables new ports much faster (sub-second) than the older protocol. **Rapid Spanning Tree** works with all Avaya equipment, and is *recommended* by Avaya.

To enable/disable spanning tree

1. Open a telnet session on the P330 stack processor, 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** to display the set spantree commands selection.

   The full set of Spanning Tree commands is displayed in Figure 23.

Figure 23: Set Spantree 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)# _
```

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 selection of Spanning Tree protocol commands displays (see Figure 23).
5. To set the **rapid spanning tree** version, type **`set spantree version rapid-spanning-tree`** and press **Enter**.

   The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order 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 by typing the CLI command **`set port spantree cost auto`**.

Note:

Avaya P330s now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop.

To set an **edge-port**, type **`set port edge admin state`** ***`module/port`*** **`edgeport`**.

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

Adjusting jitter buffers

Since network packet delay is usually a factor, jitter buffers should be no more than twice the size of the largest statistical variance between packets. The best solution is to have dynamic jitter buffers that change size in response to network conditions. Avaya equipment uses dynamic jitter buffers.

- Check for network congestion
- Bandwidth too small
- Route changes (can interact with network congestion or lack of bandwidth)

Configuring UDP ports

Communication Manager allows users to 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. Communication Manager can download default values to the endpoint when those values are not provided by the endpoint installer or the user.

About Media Encryption

This section provides information on the use and administration of Communication Manager Media Encryption. Use any of the following links to go to the appropriate section:

- What is Media Encryption?
- What are the limitations of Media Encryption?
- What types of media encryption are available?
- Is there a license file requirement?
- Administering Media Encryption
- How does Media Encryption interact with other features?
- About legal wiretapping
- About possible failure conditions

What is Media Encryption?

To provide privacy for media streams that are carried over IP networks, Communication Manager supports encryption for IP bearer channel — voice data transported in Real Time Protocol (RTP) — between any combination of media gateways and IP endpoints.

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

With media encryption enabled, Communication Manager encrypts IP packets before they 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 there are:

- No visual or audible indicators to indicate that the call is encrypted.
- No appreciable voice quality differences between encrypted calls and non-encrypted calls.

What are the limitations of Media Encryption?

⚠ **SECURITY ALERT:**
Be sure that you understand these important media encryption limitations:

1. Any call that involves a circuit-switched (TDM) endpoint such as a DCP or analog phone is vulnerable to conventional wire-tapping techniques.

2. 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 3rd-party vendor switches.

3. Any party that is not encrypting an IP conference call exposes all parties on the IP call between the unencrypted party and its supporting media processor to monitoring, even though the other IP links are encrypting.

What types of media encryption are available?

Avaya Encryption Algorithm (AEA) and Advanced Encryption Standard (AES) are supported by most Avaya IP endpoints. The Secure Real Time Protocol (SRTP) encryption standard is supported by SIP endpoints and trunks and by the 9600-series telephones.

Table 15: Media Encryption support lists the telephones and Communication Manager releases that support each type of media encryption.

Table 15: Media Encryption support

	Media Encryption Type		
	AEA	**AES**	**SRTP**
Communication Manager release	CM 1.3 and later	CM 2.0 and later	CM 4.0 and later
Avaya IP telephones:			
4601	Y	Y	N
4602	Y	Y	N
4606	Y	N	N
4610SW	Y	Y	N
4612	Y	N	N
4620	Y	Y	N
4620SW / 4621SW / 4622SW / 4625SW / 4630SW	Y	Y	N
4624	Y	N	N
4630	Y	N	N
4690	N	Y	N
1600-series IP telephones	N	Y	N
9600-series IP telephones	N	Y	Y
96xx SIP endpoints	N	N	Y
IP Softphone	Y	Y	N
IP Softphone for Windows Mobile	Y	Y	N
IP SoftConsole	Y	N	N
IP Agent	Y	Y	N
TN2302AP IP Media Processor circuit pack	Y	Y	N
TN2602AP IP Media Resource 320 circuit pack	Y	Y	Y
VoIP elements of H.248 media gateways	Y	Y	Y
Avaya one-X Communicator	N	Y	Y
OSPC	Y	N	N
Avaya 3616 / 3620 / 3626 / 3641 / 3645	N	N	N
Avaya 3631	N	Y	N

Is there a license file requirement?

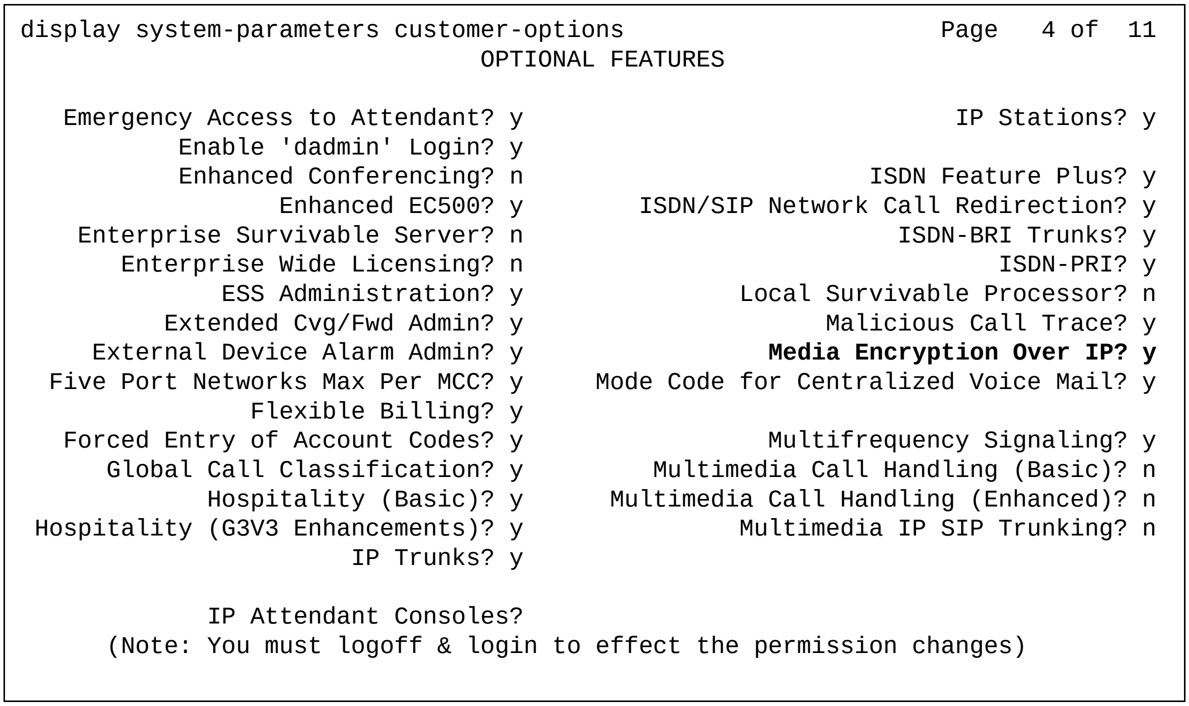
Media Encryption does not work unless the server has a valid license file with Media Encryption enabled. First check the current license file (Is Media Encryption currently enabled?) and if Media Encryption is not enabled, then you must install a license file with Media Encryption enabled.

Is Media Encryption currently enabled?

To determine whether Media Encryption is enabled in the current License File:

1. At the SAT type **`display system-parameters customer-options`** and press **Enter** to display the **Optional Features** screen.
2. Scroll to the page with the **Media Encryption Over IP?** field and verify that the value is ***y***.

Media encryption field on Optional Features screen



```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? n                        ISDN Feature Plus? y
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? y               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? y                 Media Encryption Over IP? y
  Five Port Networks Max Per MCC? y     Mode Code for Centralized Voice Mail? y
                Flexible Billing? y
   Forced Entry of Account Codes? y                 Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? n
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? n
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? n
                       IP Trunks? y

             IP Attendant Consoles?
      (Note: You must logoff & login to effect the permission changes)
```

Media Encryption is enabled to adhere to regulations established by the various national governments. Default of whether this feature is enabled or disabled is a function of the license.

Administering Media Encryption

This section contains Communication Manager administration procedures for:

- Administering Media Encryption for IP Codec Sets
- Administering Media Encryption for signaling groups

Note:
IP endpoints do not require any encryption administration, and end users do not have to do anything to use media encryption.

Administering Media Encryption for IP Codec Sets

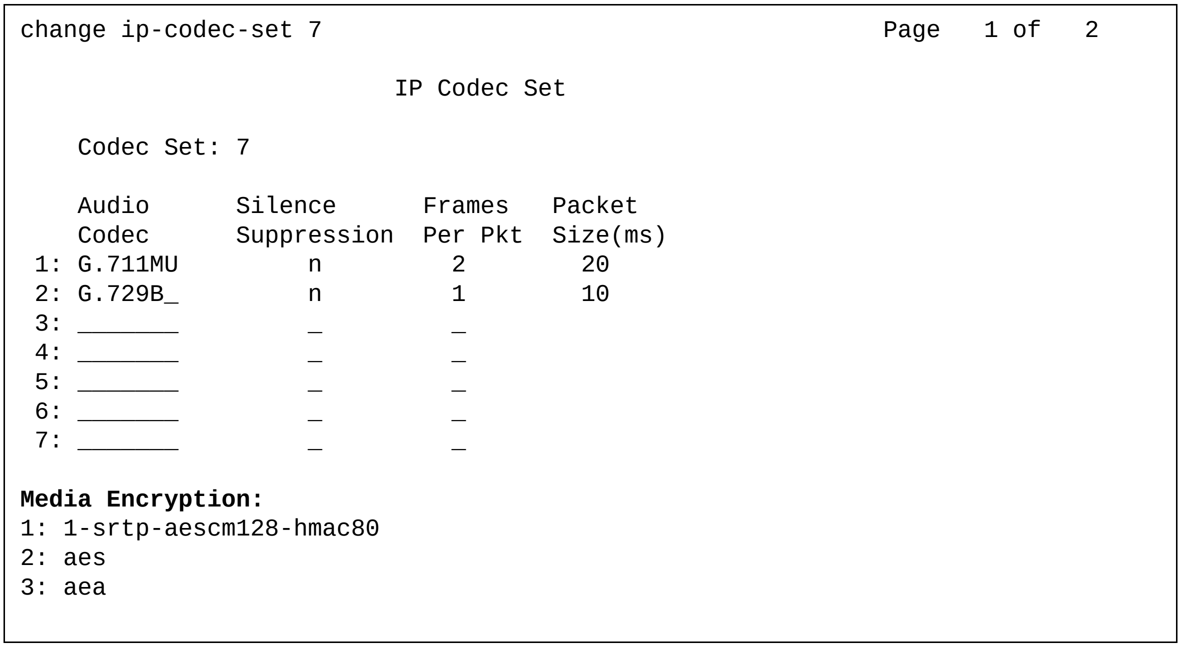
The **IP Codec Set** screen enables you to administer the type of media encryption, if any, for each codec set.

Note:
See Table 12: IP Codec Set screen fields, page 1 on page 142 for a description of the fields on the IP Codec Set screen.

To administer media encryption on an IP codec set:

1. At the SAT type **change ip-codec-set *number*** and press **Enter** to display the **IP Codec Set** screen.

Media Encryption field on the IP Codec Set screen



```
change ip-codec-set 7                                       Page   1 of   2

                          IP Codec Set

    Codec Set: 7

    Audio      Silence      Frames   Packet
    Codec      Suppression  Per Pkt  Size(ms)
 1: G.711MU         n         2        20
 2: G.729B_         n         1        10
 3: _______         _         _
 4: _______         _         _
 5: _______         _         _
 6: _______         _         _
 7: _______         _         _

Media Encryption:
1: 1-srtp-aescm128-hmac80
2: aes
3: aea
```

2. Enter up to three media encryption types listed in Table 16: Media Encryption Field Values (IP Codec Set) on page 182:

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

   Note:
   This field is hidden if the **Media Encryption Over IP?** field on the **Customer Options** screen (Media encryption field on Optional Features screen on page 180) is *n*. The **Media Encryption** field appears only if the **Media Encryption over IP** feature is enabled in the license file (and displays as *y* on the **Customer Options** screen).

The **Media Encryption** field specifies one, two, or three options for the negotiation of encryption — in this example, one of the modes of **SRTP**, **aes**, and **aea**. You can specify no encryption by entering **none** in the **Media Encryption** field. 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.

The selected options for an IP codec set applies to all codecs defined in that set.

Table 16: Media Encryption Field Values (IP Codec Set)

Valid entries	Usage
aes	Advanced Encryption Standard (AES), a standard cryptographic algorithm for use by U.S. government organizations to protect sensitive (unclassified) information. AES reduces circuit-switched-to-IP call capacity by 25%.
aea	Avaya Encryption Algorithm. AEA is not as secure an algorithm as AES but call capacity reduction with AEA is negligible. Use this option as an alternative to AES 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.
SRTP — several encryption modes	SRTP provides encryption and authentication of RTP streams for calls between SIP-SIP endpoints, H.323-H.323 endpoints, and SIP-H.323 endpoints. SIP endpoints cannot use AEA or AES encryption. See Table 12: IP Codec Set screen fields, page 1 on page 142 for a list of SRTP encryption modes.
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.

Note:

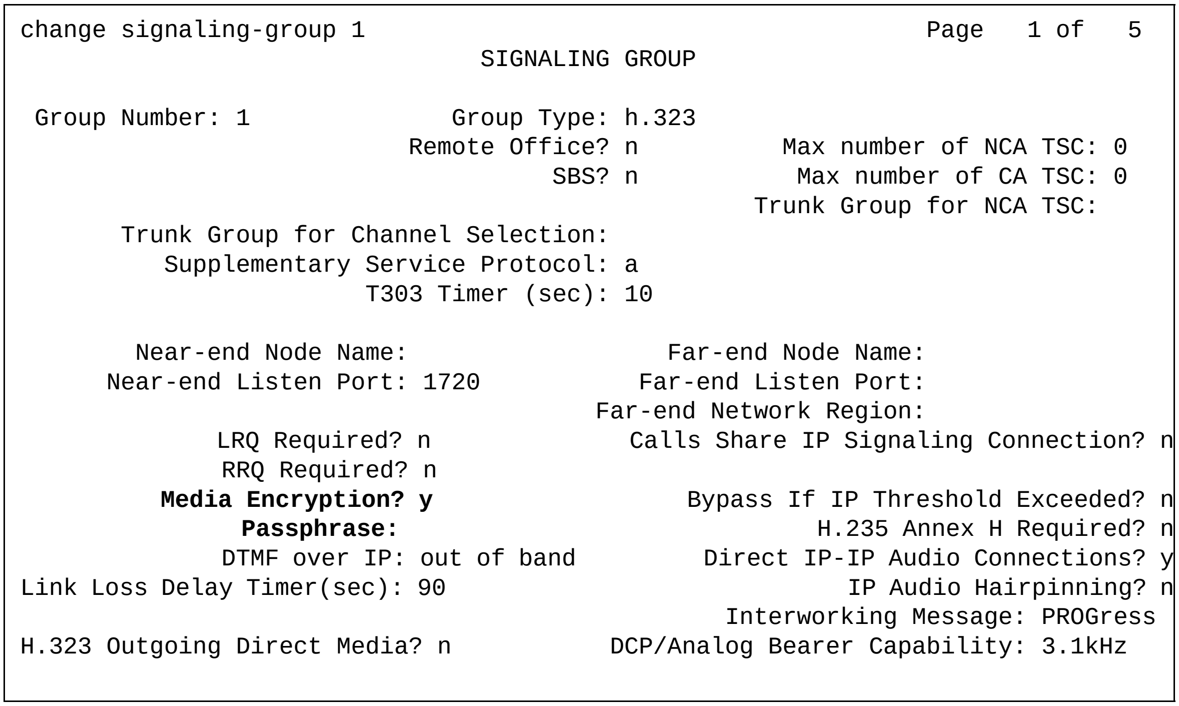
The initial default value for this field is *none* when the **Media Encryption Over IP?** field in the **Optional Features** screen (on the **Customer Options** screen) is enabled (*y*) for the first time. If this field is *n*, the **Media Encryption** field on the **IP Codec Set** screen is hidden and functions as if *none* was selected.

Administering Media Encryption for signaling groups

To administer Media Encryption for an IP signaling group:

1. At the SAT type **`change signaling-group`** ***`number`*** to display the **Signaling Group** screen

Media encryption and passphrase fields for signaling groups



```
change signaling-group 1                                       Page   1 of   5
                                SIGNALING GROUP

 Group Number: 1             Group Type: h.323
                           Remote Office? n         Max number of NCA TSC: 0
                                     SBS? n          Max number of CA TSC: 0
                                                   Trunk Group for NCA TSC:
       Trunk Group for Channel Selection:
          Supplementary Service Protocol: a
                        T303 Timer (sec): 10

        Near-end Node Name:                Far-end Node Name:
      Near-end Listen Port: 1720         Far-end Listen Port:
                                      Far-end Network Region:
              LRQ Required? n             Calls Share IP Signaling Connection? n
              RRQ Required? n
          Media Encryption? y                 Bypass If IP Threshold Exceeded? n
               Passphrase:                             H.235 Annex H Required? n
              DTMF over IP: out of band         Direct IP-IP Audio Connections? y
Link Loss Delay Timer(sec): 90                           IP Audio Hairpinning? n
                                                 Interworking Message: PROGress
H.323 Outgoing Direct Media? n          DCP/Analog Bearer Capability: 3.1kHz
```

2. Enter ***y*** in the **Media Encryption?** field to enable Media Encryption on trunk calls using this signaling group.

Note:
Leaving this field in the default state (**n**) overrides the encryption administration on the IP Codec Set screen (Media Encryption field on the IP Codec Set screen on page 181) for any trunk call using this signaling group. That is, if the IP codec set that is used between two networks is administered as **aes** or **aea** (Table 16: Media Encryption Field Values (IP Codec Set) on page 182), then a call between two endpoints over a H.323 trunk using this IP codec set fails because there is no voice path.

This field does not display if the **Media Encryption Over IP?** field is *n* on the **Customer Options** screen (Media encryption field on Optional Features screen on page 180).

3. Type an 8- to 30-character string in the **Passphrase** field.

   This string:

   - Must contain at least 1 alphabetic and 1 numeric symbol
   - Can include letters, numerals, and!&*?;'^(),.:-
   - 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, you must administer both Signaling Group forms with *exactly the same passphrase* for the A-to-B trunk connection.

   If you have previously administered a passphrase, a single asterisk (*) appears in this field. If you have not administered a passphrase, the field is blank.

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

- **Media Encryption Over IP?** field on the **Customer Options** screen (Media encryption field on Optional Features screen on page 180) is *n*.

  or

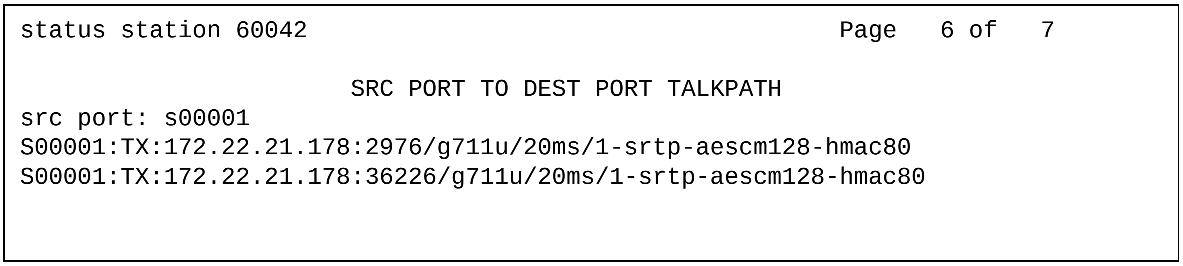
- **Media Encryption?** field on the **Signaling Group** screen (Media encryption and passphrase fields for signaling groups on page 183) is *n*.

Viewing encryption status for stations and trunks

The current status of encryption usage by stations and trunks can be viewed using the **`status station`** and **`status trunk`** commands.

To check media encryption usage for a station, enter **`status station <`*`extension`*`>`**, and go to the **Connected Ports** page.

Connected ports screen



```
status station 60042                                        Page   6 of   7

                       SRC PORT TO DEST PORT TALKPATH
src port: s00001
S00001:TX:172.22.21.178:2976/g711u/20ms/1-srtp-aescm128-hmac80
S00001:TX:172.22.21.178:36226/g711u/20ms/1-srtp-aescm128-hmac80
```

This screen shows that a port is currently connected and using a G711 codec with SRTP media encryption.

To check media encryption usage for a trunk, enter **`status trunk <`*`group/member`*`>`**.

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

About legal wiretapping

If you receive a court order requiring you to provide law enforcement access to certain calls placed to or from an IP endpoint, you can administer Service Observing permissions to a selected target endpoint (see Service Observing in Table 17: Media Encryption interactions on page 186). Place the observer and the target endpoint in a unique Class of Restriction (COR) with *exactly the same properties and calling permissions* as the original COR, otherwise the target user might be aware of the change.

About possible failure conditions

Using Media Encryption in combination with an administered security policy might lead to blocked calls or call reconfigurations because of restricted media capabilities. For example, if the IP codec set that is used between two network regions is administered as **aes** or **aea**, and if a call between two endpoints (one in each region) that do not support at least one common encryption option is set up, then there is no voice path.

How does Media Encryption interact with other features?

Media Encryption does not affect most Communication Manager features or adjuncts, except for those listed in Table 17: Media Encryption interactions on page 186.

Table 17: 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, which 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 behavior on a call varies based on these conditions at call set up: ● Whether shuffled audio connections are permitted ● Whether the call is an inter-region 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 may be carried on an H.323 trunk that is encrypted; however the T.38 packet is sent in the clear.

Network recovery and survivability

This covers the following topics:

About 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 to 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.

Two integrated management tools, Avaya VoIP Monitoring Manager and Avaya Policy Manager are briefly described in this section.

For a detailed discussion of Avaya's network management products, common third-party tools, and the distributed and centralized management models, see *Avaya Application Solutions: IP Telephony Deployment Guide* (555-245-600).

Monitoring network performance

The Avaya VoIP Monitoring Manager, a VoIP Network Quality monitoring tool, allows you to monitor these quality-affecting network factors:

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

Controlling QoS policies

Avaya Policy Manager is a network management tool that allows you to control Quality of Service (QoS) policies in your IP voice network consistently:

- Avaya Policy Manager helps you implement QoS policies consistently 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.

Figure 24 illustrates how Avaya Policy Manager works.

Figure 24: Avaya Policy Manager application sequence

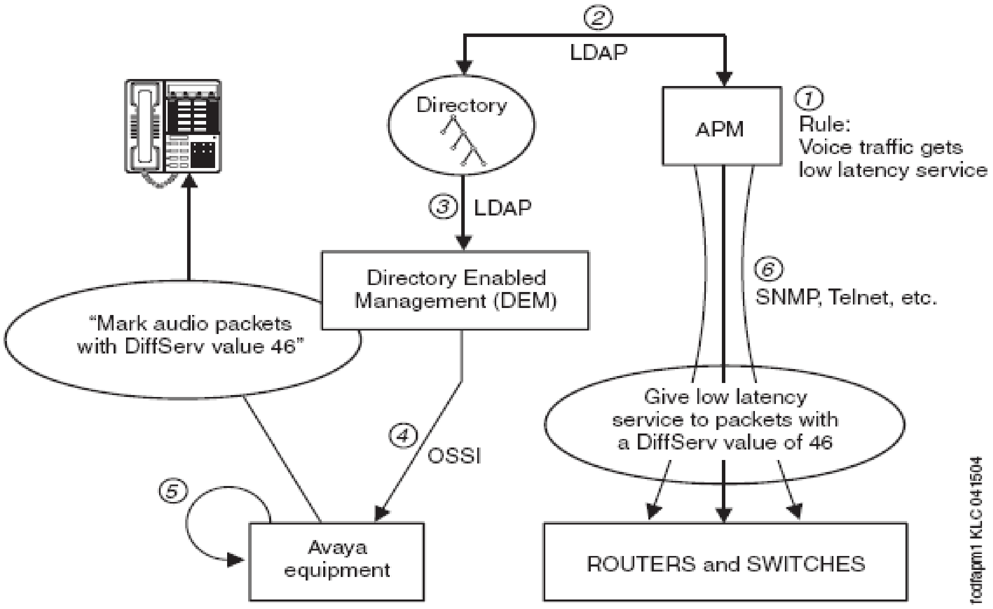


Figure notes:

1. Business rule established in Avaya Policy Manager
2. Avaya Policy Manager uses LDAP to update Communication Manager
3. Directory Enabled Management (DEM) identifies the change in the directory.
4. EDG updates Communication Manager administration through the Ethernet switch
5. Communication Manager tells the Media Processor, C-LAN, and IP Phones to mark audio packets with DSCP=46.
6. Avaya Policy Manager distributes policy information to other network devices, including low latency service for DiffServ value of 46.

For more information about Avaya Policy Manager, see your Avaya representative.

About H.248 link loss recovery

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

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

If the link goes down, Link Recovery preserves any existing calls and attempts to re-establish the original link. If the gateway/endpoint cannot reconnect to the original server/gateway, then Link Recovery automatically attempts to connect with alternate TN799DP (C-LAN) circuit packs within the original server’s configuration or to a Survivable Remote server.

Overlap with the Auto Fallback to Primary feature occurs when the Link Loss Recovery starts while the media gateway is trying to migrate back to the primary, with its new registration message indicating that service is being obtained from elsewhere.

A race condition may exist in which there is an outstanding media gateway registration to the primary while the link to the Survivable Remote server is lost. The media gateway awaits a denial or acceptance from the primary call controller. If it is an acceptance, then the Link Loss Recovery is terminated, and the media gateway is serviced by the primary call controller. If it is a denial, then the media gateway immediately sends a new registration to the primary call controller indicating no service, and the existing H.248 Link Loss Recovery feature takes over.

These features are similar in that they both attempt to return service to the primary call controller; however, Link Loss Recovery does it based upon a link failure, whereas auto fallback to primary does it based upon a working fragmented network.

Auto fallback to primary controller for H.248 media gateways

The intent of the auto fallback to primary controller feature is to return a fragmented network, in which a number of H.248 Media Gateways are being serviced by one or more Survivable Remote servers, to the primary server in an automatic fashion. This feature is targeted towards all H.248 media gateways. By migrating the media 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; unstable connections (such as ringing calls) are not. There still may be a very short interval without dialtone for new calls.

The media gateway presents a new registration parameter that indicates that Service is being obtained from an Survivable Remote server, and indicates the number of active user calls on the media gateway platform. The server administers each media gateway to have its own set of rules for Time of Day migration, enable/disable, and the setting of call threshold rules for migration.

This feature allows the administrator to define any of the following rules for migration:

- The media gateway should migrate to the primary automatically, or not.
- The media gateway should migrate immediately when possible, regardless of active call count.
- The media gateway should only migrate if the active call count is 0.
- The media gateway should only be allowed to 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 media 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 those media gateways that are currently not being serviced by an Survivable Remote server. This priority is not administrable.

There are several reasons for denying an auto-fallback, which can result from general system performance requirements, or from administrator-imposed requirements. General system performance requirements can include denial of registration because:

- Too many simultaneous media 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 media gateway in question.
- The administered minimum time for network stability has not been exceeded.

Other characteristics of this feature include:

- This feature does not preclude an older GW firmware release from working with Communication Manager 6.0 or vice versa; however, the auto-fallback feature would not be available.

  For this feature to work, the call controller is required to have Communication Manager 6.0, while the media gateway is required to have the GW firmware available at the time of the Communication Manager 6.0 release.
- Existing H.248 media gateways are the targets.

- Survivable Remote server operation is completely unaffected.

  The Survivable Remote server simply sees that a particular media gateway has lost its connection with the Survivable Remote server. The existing H.248 Link Loss Recovery algorithm on the Survivable Remote server cleans up all outstanding call records within the Survivable Remote server after the prescribed time interval.

Basic feature operation

The following steps illustrate the basic operation of the auto-fallback to primary for H.248 media gateways feature. While not exactly so, the steps are approximately sequential.

1. The media gateway/server *by default* has this feature disabled.

   If the media gateway is initially registered with an older server, the version information exchange is sufficient for the media gateway to know not to attempt to fallback to the primary automatically.

2. By means of administration on the server, this feature can be enabled for any or all media gateways controlled by that server.

   The *enable/disable* administration on the server determines whether the server will *accept/deny* registration requests containing the new parameter that service is being obtained from an Survivable Remote server. The media gateway continuously attempts to register with the server, however, even if the server has been administered never to accept the registration request (that is, the auto-fallback feature is disabled on the server). In such a case, a manual return of the media gateway is required, which generates a different registration message that is accepted by the server.

   Note:
   There is still value in receiving the registration messages when auto-fallback is disabled on the server, and that value is to see the stability of the network over time, since those messages act as "keep-alive" messages.

3. The permission-based rules that include time of day and context information are only known to the server.

   There is no need for the Survivable Remote server to have any of these translations.

4. When associated with a primary controller running Communication Manager 3.0, the media gateway attempts to register with the primary controller whenever it is connected to an Survivable Remote server.

   This registration attempt happens every 30 seconds, once the media gateway is able to communicate with the primary controller. The registration message contains an element that indicates:

   - that the media gateway is being serviced by an Survivable Remote server, and
   - the number of active user calls on that media gateway.

5. Upon the initial registration request, the primary controller initializes the encrypted TCP link for H.248 messaging.

   This is performed regardless of whether that initial registration is honored or not, and that encryption is maintained throughout the life of the registration requests. The encryption is also maintained once a registration is accepted by the primary controller. Encryption of the signaling link is performed at the outset during this automatic fallback process to ensure the security of the communication between the primary call controller and the media gateway.

6. The primary controller, based upon its administered rules, may allow or deny a registration.

   If the primary controller gets a registration message without Service State information, for example, an older media gateway, or if a new media gateway states it does not have service, then the primary honors those registration requests above all others immediately.

7. If the registration is denied, the media gateway continues to send the registration message every 30 seconds, which acts as a *de facto* '"keep-alive" message.

8. The media gateway constantly monitors the call count on its platform, and asynchronously sends a registration message whenever 0 context is achieved.

9. Once the registration message is accepted by the primary, then the H.248 link to the Survivable Remote server is dropped.

Split registration prevention

Split registration occurs when resources in one network region are registered to different servers. For example, aftet an outage activates Survivable Remote Servers, telephones in a network region register to the main server or Survivable Core Servers, while the gateways are registered on the Survivable Remote Server. The telephones registered with the main server are isolated from their trunk and VOIP resources.

The split registration prevention solution enables the administrator to manage system behaviour after an outage. The administrator can force telephones and gateways to register with the main server or the Survivable Remote Server. For more information on split registration prevention, see *Administering Avaya Aura ^{TM} Communication Manager, 03-300509*.

G250 interworking

When calls are made on the media gateway while it is controlled by the Standard Local Survivability (SLS) , the G250, G350, G430 and G450 behave as any Survivable Remote server might behave. The SLS mode using its administration and dial analysis plan, can allow local calls to be established from:

- Local station to or from local station (analog or registered IP) . Supports analog, DCP, and H.323 IP phones.

- Local station to or from local analog two-way CO trunks. Supports two-way Loop -Start and Ground-Start analog trunks supports analog did trunks, supports Basic Rate ISDN trunks, supports Primary rate ISDN trunks, supports T1-Robbed Bit and E1-CAS digital non-ISDN trunks.
- Digital non-ISDN trunks support the following signaling supervision types:
  - loop-start
  - ground-start
  - wink-wink
  - wink-immediate
  - wink-auto
  - immediate-immediate
  - auto-auto
  - auto-wink

While operating in SLS mode, the media gateway attempts to re-register with the primary controller on its MGC list. As soon as the gateway is able to re-register with the primary controller, it un-registers with SLS, and re-registers with the primary controller. In terms of re-registration with the primary controller, the Auto Fallback to Primary feature would therefore work in a similar way with the media gateway SLS as it does with the Survivable Remote servers in the G350 or G700.

Note:
The connection preserving aspects of this feature will not be available 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 denial cause for the rejection of the new registration message. Given that the G350 was only introduced in the Communication Manager 2.0 timeframe, it is not backwards compatible with previous Communication Manager releases.

In a startup scenario, there is an exchange of version information between Communication Manager and the media gateway. If the Communication Manager load is pre-Communication Manager 3.0, then the auto-fallback mechanism remains disabled for the media gateway. Any subsequent registration with a primary controller (from the MGC list) that is running release Communication Manager 3.0 results in the auto fall-back feature being enabled for the media gateway.

The only time when the media gateway may send a registration message to an older primary call controller is in the rare case when the primary controller has been downgraded while the media gateway has been receiving service from an Survivable Remote server. In this case, the media gateway receives a protocol error that can be used to send a registration message consistent with Communication Manager 2.0. Downgrading to earlier than Communication Manager 2.0 with a G350 would result in the G350 not being able to register at all.

G700 interworking

The G700 Media 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 NSD (Non-Standard Data) expansion with the OID is used to carry the context count.

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

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

Though not directly necessary for this feature, the media gateway responds to any of the aforementioned protocol errors by attempting to register with the lowest common denominator registration message. This allows new media gateways to be backward compatible with even older releases. This modification only applies to the G700.

Older media gateway loads

The auto-fallback feature on the server is passive in nature; therefore, an older media gateway load trying to register with the current Communication Manager load registers with priority, since the value of the Service-State is that of a media gateway without service. Any defined rules for the media gateway are ignored, given that an older media gateway firmware release tries to register only when it no longer has service from another server; therefore, the administration of rules for old media gateway firmware loads are irrelevant.

Administering auto fallback to primary

For each media gateway, the following administration must be performed:

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

Adding Recovery Rule to Media Gateway screen

The **Media Gateway** screen (**`change media-gateway`** ***n***) has a field called **Recovery Rule** with the following attributes:

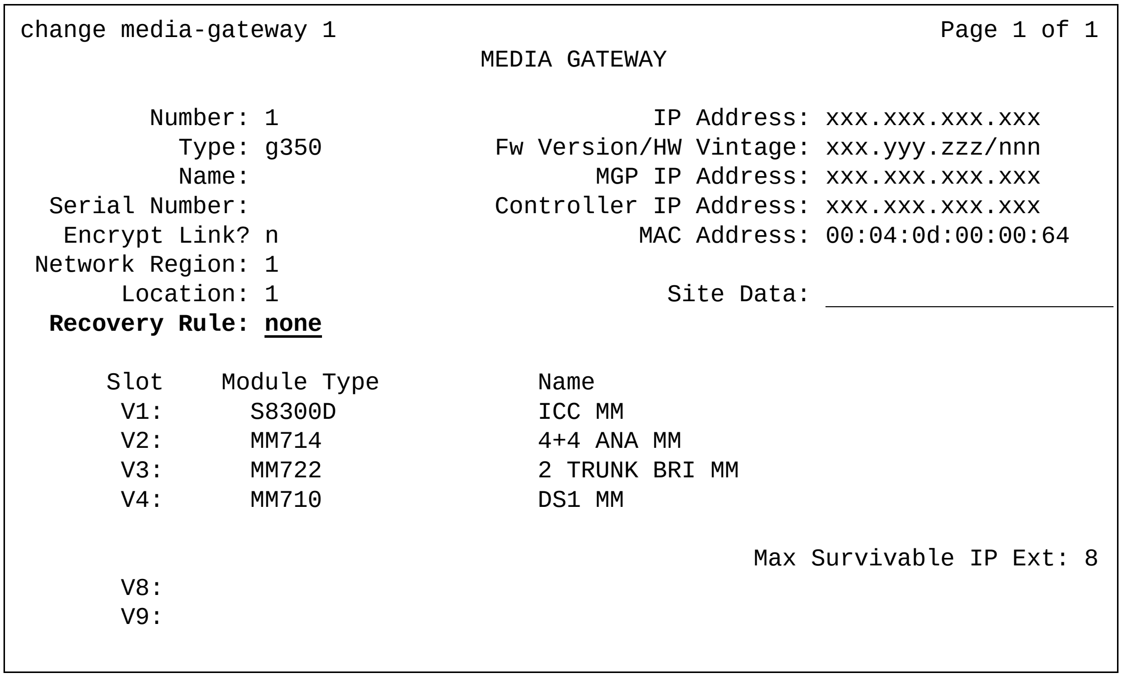
- Acceptable values for the field are **none**, **1 - 50**, or **1 - 250**, where
  - **50** is the maximum number of supported media gateways on an S8300D Server, and
  - **250** is the maximum number of supported media gateways on a standalone server.
- Default is **none**, which indicates that no automatic fallback registrations will be accepted.
- The value of **1 - 50**, or **1 - 250** applies a specific recovery rule to that numbered gateway.

Note:
A single recovery rule number may be applied to all media gateways, or each media gateway may have its own recovery rule number, or any combination in between.

By associating the recovery rule to the **Media Gateway** screen (see Figure 25), an administrator can use the **`list media-gateway`** command to see which media gateways have the same recovery rules. All the administration parameters for the media gateways are consolidated on a single screen. The actual logic of the recovery rule is separate, but an administrator can start from the Media Gateway screen and proceed to find the recovery rule.

Note:
These changes apply to the **`display media-gateway`** command, as well.

Figure 25: Media Gateway screen



```
change media-gateway 1                                          Page 1 of 1
                                MEDIA GATEWAY

         Number: 1                          IP Address: xxx.xxx.xxx.xxx
           Type: g350            Fw Version/HW Vintage: xxx.yyy.zzz/nnn
           Name:                        MGP IP Address: xxx.xxx.xxx.xxx
  Serial Number:                 Controller IP Address: xxx.xxx.xxx.xxx
   Encrypt Link? n                         MAC Address: 00:04:0d:00:00:64
 Network Region: 1
       Location: 1                           Site Data: ____________________
  Recovery Rule: none

      Slot    Module Type           Name
       V1:      S8300D              ICC MM
       V2:      MM714               4+4 ANA MM
       V3:      MM722               2 TRUNK BRI MM
       V4:      MM710               DS1 MM

                                                   Max Survivable IP Ext: 8
       V8:
       V9:
```

In the above example, no automatic fallback registration requests will be accepted by the primary controller for Media Gateway 1 when it is active on an Survivable Remote server.

Note:
For more detailed descriptions of the entries and values fields on this screen, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431, at http://www.avaya.com/support).

Administering the System Parameters Media Gateway Automatic Recovery Rule screens

Definition of recovery rules occurs on the **System Parameters Media Gateway Automatic Recovery Rule** screens (**`change system-parameters mg-recovery-rule <`*`n`*`>`**. This screen is contained within the 'system-parameters' area of administration screens. The maximum number of screens that can be administered correspond to the maximum number of media gateways supported by the server in question, and are:

- Up to 50 for the S8300D Server
- Up to 250 for the standalone Servers

These screens provide a field, **Migrate H248 MG to primary**, with 4 administrable options:

Note:
For detailed information on all four options, see *Administering Avaya Aura™ Communication Manager,* 03-300509.

1. **immediately** — which means that the first media gateway registration that comes from the media gateway is honored, regardless of context count or time of day.

   The Warning displayed in Figure 26 is visible when a user selects this option. This option is the default for all rules.

2. **0-active calls** — which means that the first media gateway registration reporting “0 active calls” is honored (see Figure 27).

3. **Time-day-window** — means that a valid registration message received during any part of this interval is honored (see Figure 28).

   Note:
   Time of day is local to the media gateway.

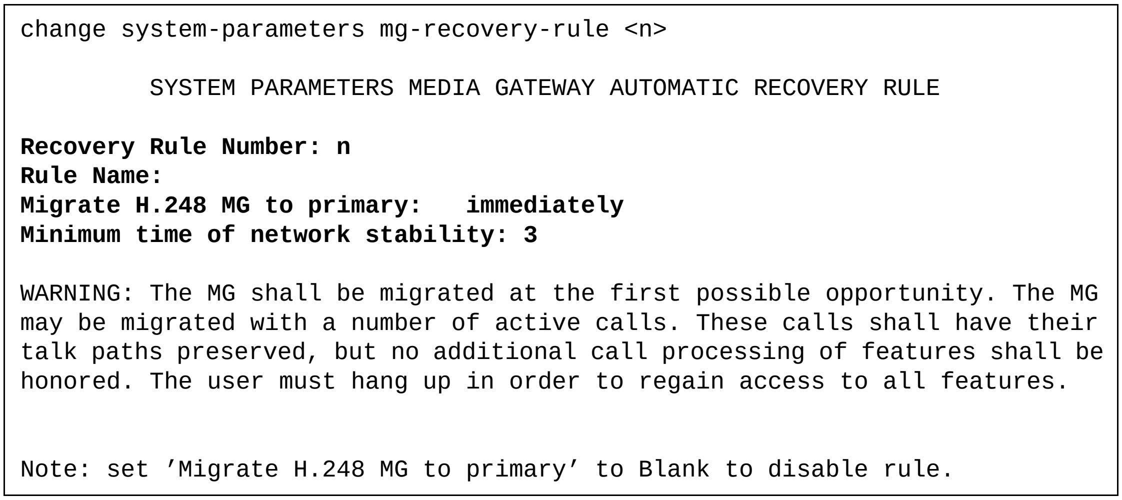
   There are no constraints on the number of active calls. The time scale provided for each day of the week goes from 00-23 hundred hours (military time). The user must specify an ‘x’ or ‘X’ for each hour where they want to permit the return migration. If they do not want to permit a given hour, then they leave it blank. This method gets around overlapping time issues between days of the week. Users can specify as many intervals as they wish.

4. **Time-window-OR-0-active-calls** — means that a valid registration is accepted *anytime,* when a 0 active call count is reported OR if a valid registration with *any* call count is received during the specified time/day intervals (see Figure 29).

Note:
Time of day is local to the media gateway.

The time scale provided for each day of the week goes from 00-23 hundred hours (military time). The user must specify an ‘x’ or ‘X’ for each hour where they want to permit the return migration. If they do not want to permit a given hour then they leave it blank. This method gets around overlapping time issues between days of the week. Users can specify as many intervals as they wish.

Figure 26: System-parameters mg-recovery-rule screen: immediately



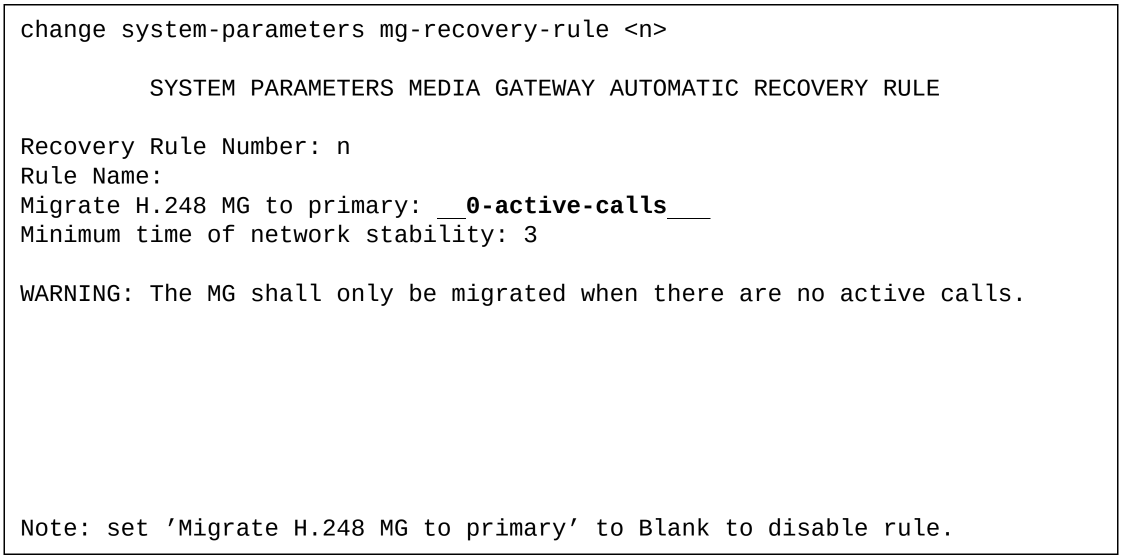
```
change system-parameters mg-recovery-rule <n>

         SYSTEM PARAMETERS MEDIA GATEWAY AUTOMATIC RECOVERY RULE

Recovery Rule Number: n
Rule Name:
Migrate H.248 MG to primary:   immediately
Minimum time of network stability: 3

WARNING: The MG shall be migrated at the first possible opportunity. The MG
may be migrated with a number of active calls. These calls shall have their
talk paths preserved, but no additional call processing of features shall be
honored. The user must hang up in order to regain access to all features.


Note: set ’Migrate H.248 MG to primary’ to Blank to disable rule.
```

Administer the following fields:

Field	Description
Recovery Rule Number	The number of the recovery rule: ● Up to 50 for the S8300D Server ● Up to 250 for the standalone servers
Rule Name	Optional text name for the rule, to aid in associating rules with media gateways.
Migrate H.248 MG to primary	One of 4 administrable options.
Minimum time of network stability	Administrable time interval for stability in the H.248 link before auto-fallback is allowed. Between 3-15 minutes (Default is 3 minutes).

Figure 27 shows the screen for the **0-active calls** option.

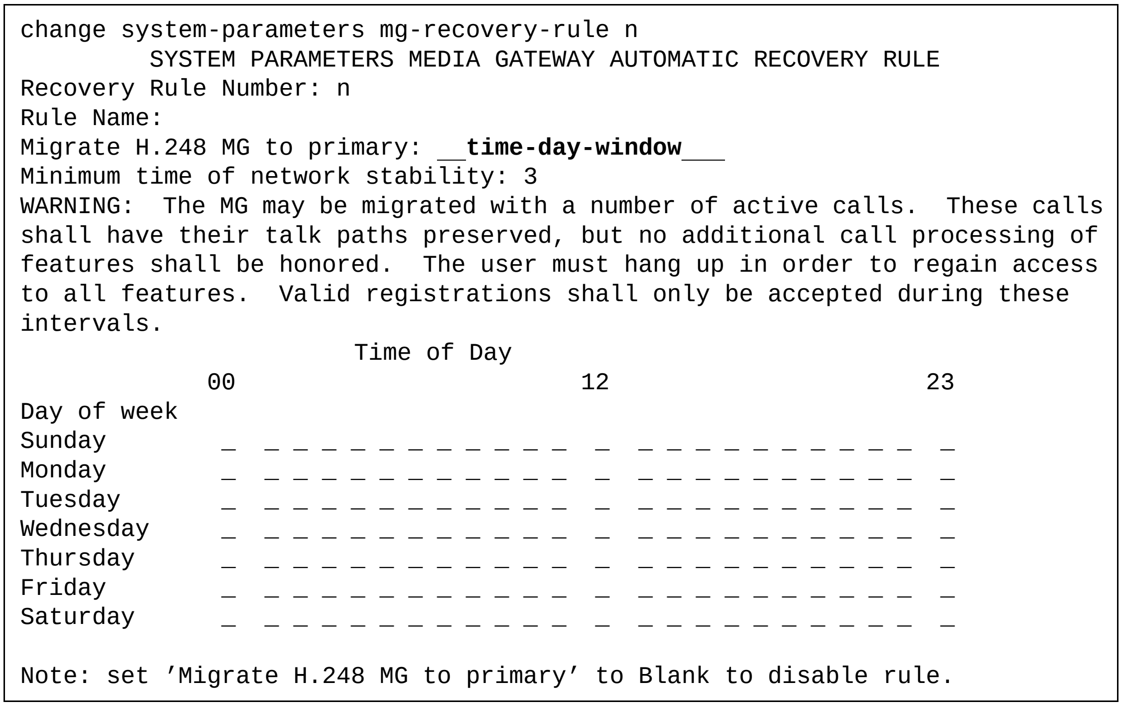
Figure 27: System-parameters mg-recovery-rule screen: 0-active calls



```
change system-parameters mg-recovery-rule <n>

         SYSTEM PARAMETERS MEDIA GATEWAY AUTOMATIC RECOVERY RULE

Recovery Rule Number: n
Rule Name:
Migrate H.248 MG to primary: __0-active-calls___
Minimum time of network stability: 3

WARNING: The MG shall only be migrated when there are no active calls.








Note: set 'Migrate H.248 MG to primary' to Blank to disable rule.
```

Figure 28 shows the screen for the time-day-window option.

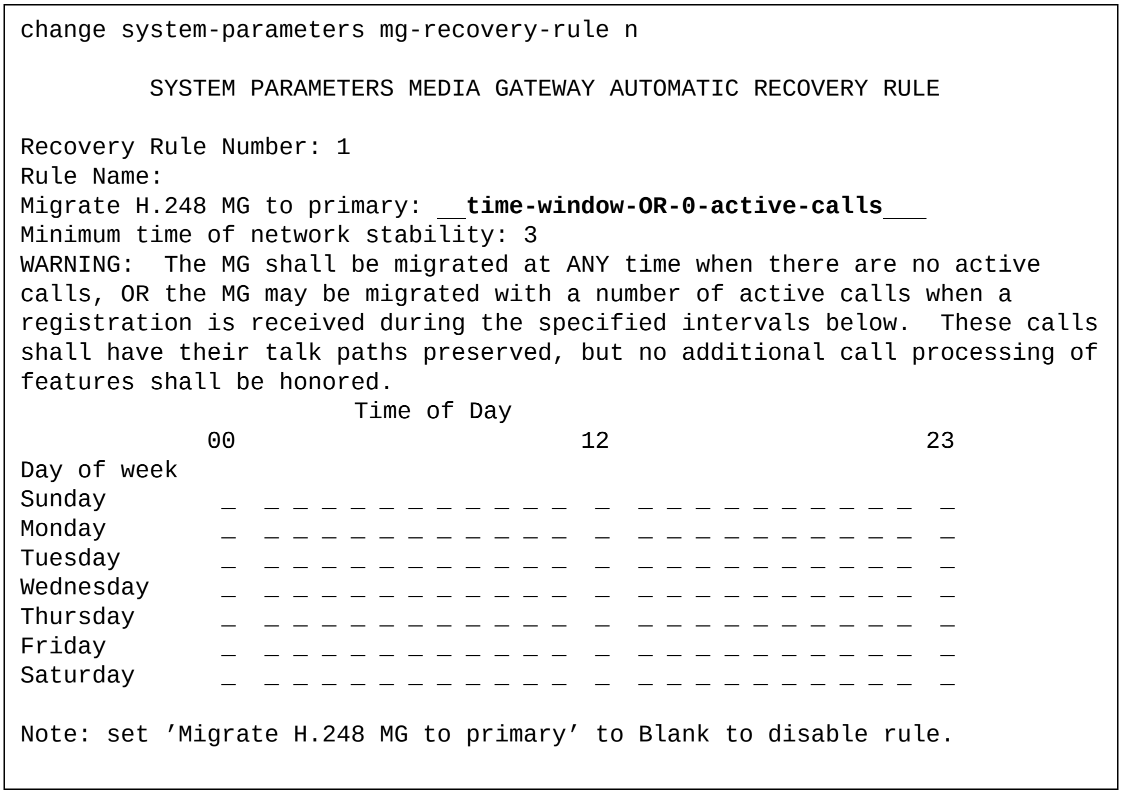
Figure 28: System-parameters mg-recovery-rule screen: time-day-window



```
change system-parameters mg-recovery-rule n
         SYSTEM PARAMETERS MEDIA GATEWAY AUTOMATIC RECOVERY RULE
Recovery Rule Number: n
Rule Name:
Migrate H.248 MG to primary: __time-day-window___
Minimum time of network stability: 3
WARNING:  The MG may be migrated with a number of active calls.  These calls
shall have their talk paths preserved, but no additional call processing of
features shall be honored.  The user must hang up in order to regain access
to all features.  Valid registrations shall only be accepted during these
intervals.
                       Time of Day
             00                        12                      23
Day of week
Sunday        _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Monday        _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Tuesday       _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Wednesday     _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Thursday      _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Friday        _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Saturday      _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _

Note: set 'Migrate H.248 MG to primary' to Blank to disable rule.
```

Figure 29 shows the screen for the **time-window-OR-0-active-calls** option.

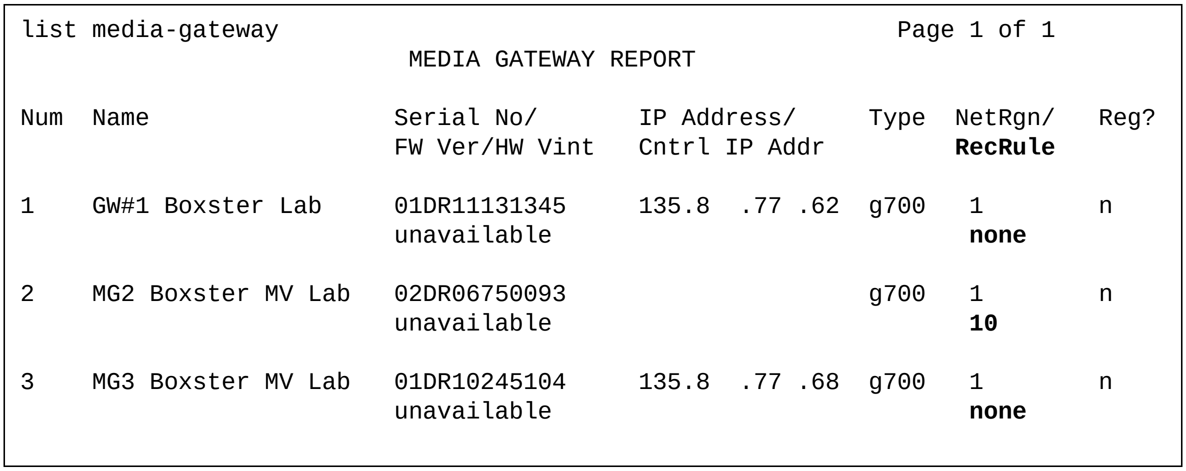
Figure 29: System-parameters mg-recovery-rule screen: time-window-OR-0-active-calls



```
change system-parameters mg-recovery-rule n

         SYSTEM PARAMETERS MEDIA GATEWAY AUTOMATIC RECOVERY RULE

Recovery Rule Number: 1
Rule Name:
Migrate H.248 MG to primary: __time-window-OR-0-active-calls___
Minimum time of network stability: 3
WARNING:  The MG shall be migrated at ANY time when there are no active
calls, OR the MG may be migrated with a number of active calls when a
registration is received during the specified intervals below.  These calls
shall have their talk paths preserved, but no additional call processing of
features shall be honored.
                       Time of Day
             00                        12                       23
Day of week
Sunday        _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Monday        _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Tuesday       _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Wednesday     _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Thursday      _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Friday        _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _
Saturday      _  _ _ _ _ _ _ _ _ _ _ _  _  _ _ _ _ _ _ _ _ _ _  _

Note: set ’Migrate H.248 MG to primary’ to Blank to disable rule.
```

For administrators to see how the recovery rules are applied across all media gateways, the **Media Gateway Report** screen (**`list media-gateway`** command) identifies the recovery rule for each media gateway in the network (See Figure 30).

Figure 30: list mg-recovery screen



```
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
```

In this example, media gateways #1 and #3 are administered such that no registration request would be accepted by the primary controller when the media gateway is active on an Survivable Remote server. Media gateway #2, on the other hand, is administered with Recovery Rule #10. The SAT command:

```
display system-parameters mg-recovery-rule 10
```

would show the details of that specific recovery rule.

Administrable IPSI Socket Sanity Timeout

The IPSI Socket Sanity Timeout provides a link-bounce type of interval between Communication Manager and the IPSI to provide resiliency during short network outages. During normal operations, Communication Manager determines the health of a connection to an IPSI by monitoring 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 (three to 15 seconds) set by an administrator for the IPSI Socket Sanity Timeout. The administered value of the IPSI Socket Sanity Timeout is the amount of time Communication Manager waits for communication to the IPSI to be restored before a recovery action is initiated. If the value for the IPSI Socket Sanity Timeout is properly engineered, the IPSI is less prone to warm starts and more resilient to short network outages.

If the value of the IPSI Socket Sanity Timeout is greater than three and if there are more than three sanity failures, the port network (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. In a suspended state all messages sent from call processing to the PN and all messages sent from the PN to call processing are delayed until communication resumes. The PN will not go into a suspended state if the value for the IPSI Socket Sanity Timeout is equal to three or if the sanity failures is less than three.

If communication is restored between the server and the IPSI before the value set for the IPSI Sanity Timeout elapses, no action is taken and 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 re-connect to the IPSI. It the attempts to reconnect are successful, the PN resets. The type of reset is dependent on the length of the outage. If communication is restored within one minute a WARM restart is performed, after one minute a COLD restart is performed.

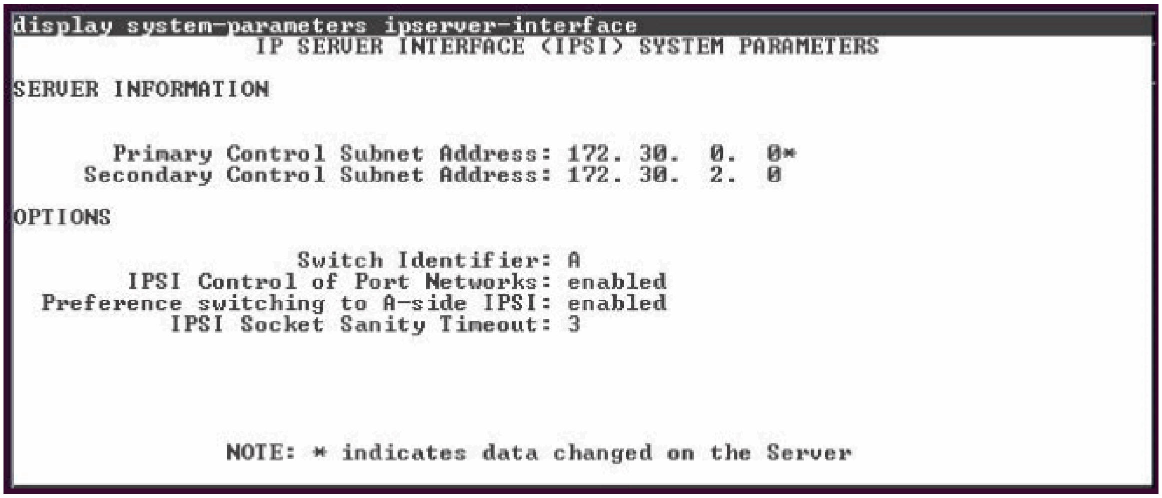
For customers upgrading to the latest release of Communication Manager with a value set by Avaya Services other than the three second default, the value set by Avaya Services is carried over during the upgrade.

Note:

The value administered for the IPSI Socket Sanity Timeout has no impact on the Survivable Core server no 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 three to 15 seconds with the default set at three seconds.

Figure 31: system-parameters ipserver-interface



```
display system-parameters ipserver-interface
                 IP SERVER INTERFACE (IPSI) SYSTEM PARAMETERS

SERVER INFORMATION


       Primary Control Subnet Address: 172. 30.  0.  0*
     Secondary Control Subnet Address: 172. 30.  2.  0

OPTIONS

                    Switch Identifier: A
        IPSI Control of Port Networks: enabled
  Preference switching to A-side IPSI: enabled
           IPSI Socket Sanity Timeout: 3





               NOTE: * indicates data changed on the Server
```

Survivable Core Servers

The Survivable Core Servers feature provides survivability to port networks by allowing backup servers to be placed in various locations in the customer's network. The backup servers supply service to port networks in the case where the main server or connectivity to the main Communication Manager server(s) is lost. Survivable Core servers offer full Communication Manager functionality when in survivable mode, provided sufficient 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 they can reach over an IP-connected network.

  That is, Survivable Core servers connected on an enterprise's public IP network will not be able to control port networks connected to control network A or B, unless:

  – Control networks A or B are exposed to the public IP network through control network on the Customer's LAN (CNOCL).

- Multiple Survivable Core servers can be deployed in a network. In the case above, an enterprise could deploy one or more Survivable Core servers on the public network, and an additional server on control networks A and B to backup port networks attached to the respective networks.

  However, when port networks register with different Survivable Core servers, system fragmentation may occur. In that case, care should be taken to establish adequate routing patterns to allow users at a particular location to be able to place calls where needed.
- Survivable Core servers register to the main server(s) through a C-LAN. Each Survivable Core server must be able to communicate with a processor Ethernet in order 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 server(s) (pre-Release 3.0)
  - TCP/21874 – Main server sends translations to the Survivable Core server (Release 3.0 and above; also for Survivable Remote server translations)

The media gateway cannot distinguish between registration through a C-LAN or registration to an S8300D directly. When a media gateway completes a successful registration through an IP address defined as a primary call controller address, if that address is a C-LAN, the media gateway may not necessarily be registered with the true primary call controller. The port network that houses the C-LAN may be under control of an Survivable Core server, but the media gateway will not know that it is registered with an Survivable Core server.

When the traditional port network migrates back to the primary call controller, then the media gateway loses its H.248 link, and the Link Loss Recovery algorithm engages, and that should be sufficient. The Auto Fallback to Primary feature only engages if the media gateway drops the connection and registers with an Survivable Remote server. The Survivable Core server migration should only occur if the port network is reasonably certain to return to the primary call controller, so the media gateway would simply return to the same C-LAN interface. Now, when the media gateway returns to the same C-LAN interface, the Link Loss Recovery feature performs a context audit with the primary controller and learns that the primary call controller is not aware of the media gateway. The controller in this case issues a warm start request to the media gateway, or potentially different behavior if connection preservation is active at the same time. The auto-fallback feature is not affected by Survivable Core server.

For more information on Survivable Core server, 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 experience disproportionately long outages from short network disruptions. The improved port network recovery feature now provides customers using IP connected Port Networks with less downtime in the face of IP network failures.

The feature lessens the impact of network failures by:

- Improving TCP recovery times that increase the IPSI-PCD socket bounce coverage time from the current 6-8 seconds range for the actual network outage to something closer to 10 seconds. Results vary based on traffic rates.
- Modifying the PKTINT recovery action after a network outage to entail a warm interrupt rather than a **PKTINT application reset** (hardware interrupt)). This prevents H.323 IP telephones from having to re-register and/or have their sockets regenerated. This minimizes recovery time from network outages in the range of 15-60 seconds.

This feature also monitors the IPSI-PCD socket and helps in identifying and troubleshooting network related problems.

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

During the network outage, only stable calls already in progress have their bearer connections preserved. A call for which the talk path between the parties in the call has been established is considered stable. Call control is not available during the network outage, and this means that any call in a changing state is most likely not preserved.

Some examples are:

- Calls with dial tone
- Calls in dialing stage
- Calls in ringing stage
- Calls transitioning to/from announcements
- Calls transitioning to/from music-on-hold
- Calls on hold
- Calls in ACD queues
- Calls in vector processing

Further, no change in the state of a preserved call is possible. So, features such as conference or transfer are not available on the preserved calls. Button pushes are not recognized. Invocation of a feature by the user is given denial treatment. In a conference call, if a party in the call drops, the entire call is dropped.

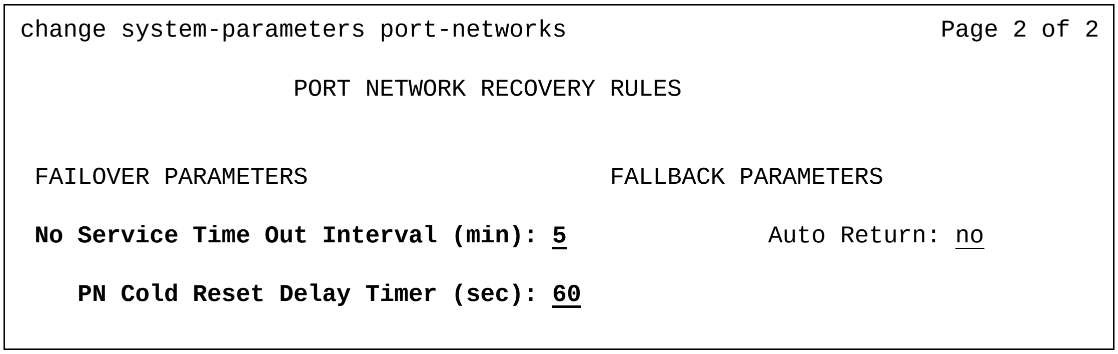
The following are additional improvements:

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

With the introduction of a warm interrupt of the PKTINT instead of reset in the 15-60 seconds range, and the optional extension of the PN cold reset from 60 to 120 seconds.

Port Network Recovery Rules screen

Figure 1: PN Cold Reset Delay Timer



```
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
```

No Service Time Out Interval

Field description

Valid entries	Usage
2 - 15	No Service Time Out Interval in minutes

PN Cold Reset Delay Timer (sec)

Field description

Valid entries	Usage
60 -120 secs	PN Cold Reset Delay Timer in seconds. The default is 60 seconds

Configuration impacts on availability

Communication Manager reduces the downtime experienced by port networks after a short network outage. H.323 endpoint and application link and socket stability is greatly improved in the sub-60 second range. H.323 endpoints using TTS will not have to regenerate sockets, and H.323 endpoints not using TTS will not have to re-register or have their sockets regenerated.

Survivability

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

Index